pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

Information Technology Policy

Access Management and Control

ITP Number	***Effective Date***
GEN-SEC013C	September 7, 2006
Category	***Supersedes***
Recommended Policy	
Contact	***Scheduled Review***
RA-ITCentral@pa.gov	Annual

1. Introduction

There are two kinds of commonwealth-managed assets that users need access to:

1. Physical assets like buildings or emergency response sites.
   - Fundamental to the physical access policy is the use of credentials.
   - The primary credential for commonwealth employees is the Employee Identity Card. GEN-SEC013E - *Specification for a Commonwealth Personal Identity Verification Card,* describes the specification for a Commonwealth Personal Identity and Verification (PIV) card that is federally compliant and compatible with most facility Access Control Systems (ACS) operated by the commonwealth.
2. Logical assets like Web sites and data systems.
   - Fundamental to the logical access policy is a shared authentication service for access to commonwealth Web sites.
   - The foundation of the Web access architecture is an Enterprise Web Access Management (EWAM) system for protecting the Enterprise Portal, including federation services (via the Security Assertion Markup Language (SAML) 2.0 standard) to provide users with access into the various agency online resources.

Inappropriate or fraudulent access to commonwealth assets exposes the commonwealth to significant risk from malicious attack. In an attempt to uniformly improve access security, the commonwealth has established policy that sets minimum proofing standards for various levels of identity trust, and a common credentialing system that can be uniformly accepted by all commonwealth agencies. The purpose of this document is to define this Access Management and Control policy, as established in ITP-SEC013 - *Identity Protection and Access Management (IPAM) Architectural Standard – Identity Management Services.*

The process of gaining access to a secured commonwealth asset consists of three steps: identification, authentication, and authorization. The first step consists of identity verification and credentialing, verifying that the user is who he or she claims to be and then issuing credentials to that effect. A credential is anything that provides the basis for confidence. It can be something the user knows (e.g., password or personal ID number), something the user carries (e.g., personal identity verification [PIV] card), or something the user is (i.e., a biometric such as a fingerprint). The second step is authentication of the user, verifying that the user

matches the credentials he or she has presented. The final step is authorization of the user, which is verifying that the user holds permission to access the secured asset. Authorization may be determined via a number of factors, such as a specific attribute of the identity (like job classification), membership in a group, or even the time of day access is attempted.

The primary focus of this document is on authentication. Identification involves the processes required to verify a user's identity, and is explored fully in GEN-SEC013D - *Enrollment, Identity Proofing and Vetting*. Authorization involves the actions that are permitted for a user once authentication has occurred. Decisions concerning authorization are to remain the purview of the business process and owner of the secured asset. However, depending on the potential risk rating of the asset, a minimum assurance level of any authorized user's authentication is in order.

1.1 Organization

After this Introduction, this document provides the following information:

- Section 2 provides a general discussion of authentication and its relationship to identity assurance.
- Section 3 defines the Shared Authentication Service architecture, which primarily leverages Web Access Management (WAM) technologies and federation via the SAML 2.0 open standard.
- Section 4 provides additional architectural details on WAM, both for the enterprise-based Shared Authentication Service and as guidance to the agencies and Communities of Practice for their local implementations.
- Section 5 provides additional architectural details on federation, both for the enterprise-based Shared Authentication Service and as guidance to the agencies and Communities of Practice for their local implementations.
- Section 6 describes the WAM and Shared Authentication Service governance model and administration structure.
- Section 7 establishes the policy governing use of a Commonwealth PIV card as an authentication credential for accessing secured assets.
- Section 8 discusses interoperability with federal standards.

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

2. Authentication and Identity Assurance

Authentication is all about confirmation of one's identity. There are two types of identity assurance associated with accessing a secured asset: assurance that the identity is who he claims to be, and assurance that the identity's access credentials are his own.

The first type of identity assurance is referred to as an identity's *Assurance Level*. This *Assurance Level* denotes the degree of assurance we have that this person is the one he or she claims to be, and it reflects the level of scrutiny applied during the identity proofing or vetting process used. It is generally performed only once for any given identity, usually in conjunction with identity card issuance. The *Assurance Level* equates to the trust level we have that the

person being granted the identity credentials is in fact the identity claimed. By having a common process for determining *Assurance Levels*, commonwealth issued credentials can share a common level of trust by all agencies and groups across the enterprise. These credentials can be used to *authenticate* the holder's identity to the WAM or other Access Management Systems (ACS) used. The minimum requirements for establishing these Assurance Levels are provided in GEN-SEC013D.

The second type of identity assurance is called the *Strength of Authentication*. It relates to the authentication method required to validate the credentials of a person seeking egress to a particular secured commonwealth asset, and is performed every time that person tries to initiate access. The *Strength of Authentication* correlates to the level of trust that the person attempting access is in fact the person to whom the credentials were issued (i.e., that the credentials have not been stolen or otherwise improperly obtained).

There are generally three ways to authenticate oneself: through something you know, something you have, or something you are. These methods can be applied individually, or combined to formulate stronger forms of authentication; for instance:

- Knowing a key code or personal identification number (PIN) to access an asset is a simple level of authentication, because only those authorized for access are to have had knowledge of that key code. But I could easily share that code with another, or someone might observe me entering the code and fraudulently learn it that way.

- A stronger form of authentication might be for me to use a personal identity verification (PIV) card, something I have, for authenticating myself. Even so, if the card were borrowed or stolen, it could provide an unauthorized person with a means to falsely authenticate his self to the asset.

- An even stronger authentication mechanism would be to require both a PIV card *and* a PIN, something I both have *and* know. This is an example of two-factor authentication. Even if the PIV card were stolen, it would be ineffective without the PIN; and likewise, knowing the PIN is insufficient without also possessing the card.

- The strongest form of authentication involves biometrics (something you are), like a fingerprint or facial image, since these can be neither stolen nor memorized.

Strength of Authentication requirements for an asset correspond to that asset's security level; that is, the importance of the asset to the organization, the asset's susceptibility to threat, and the potential harm that could result were a security breach to occur. Just as each agency is responsible for providing the local authorization service to allow access to each of their secured resources, they are also responsible for determining the security levels of their assets and the appropriate *Strength of Authentication* required to access them. ITP-SEC005 - *Commonwealth Application Certification and Accreditation* describes the process for conducting a security assessment.

There is a correlation between a user's *Assurance Level* and the asset's security level. *Assurance Level* requirements need to be more stringent for assets with higher authentication strength requirements. Authorization to the asset is to be approved only for users who have been vetted to an *Assurance Level* at least as high as the minimum requirement assigned to that asset.

3. Shared Authentication Service

The IPAM initiative establishes a Shared Authentication Service for the various agencies in the commonwealth. This section details the architecture of that service, as shown in Figure 1 – Shared Authentication Service Architecture.

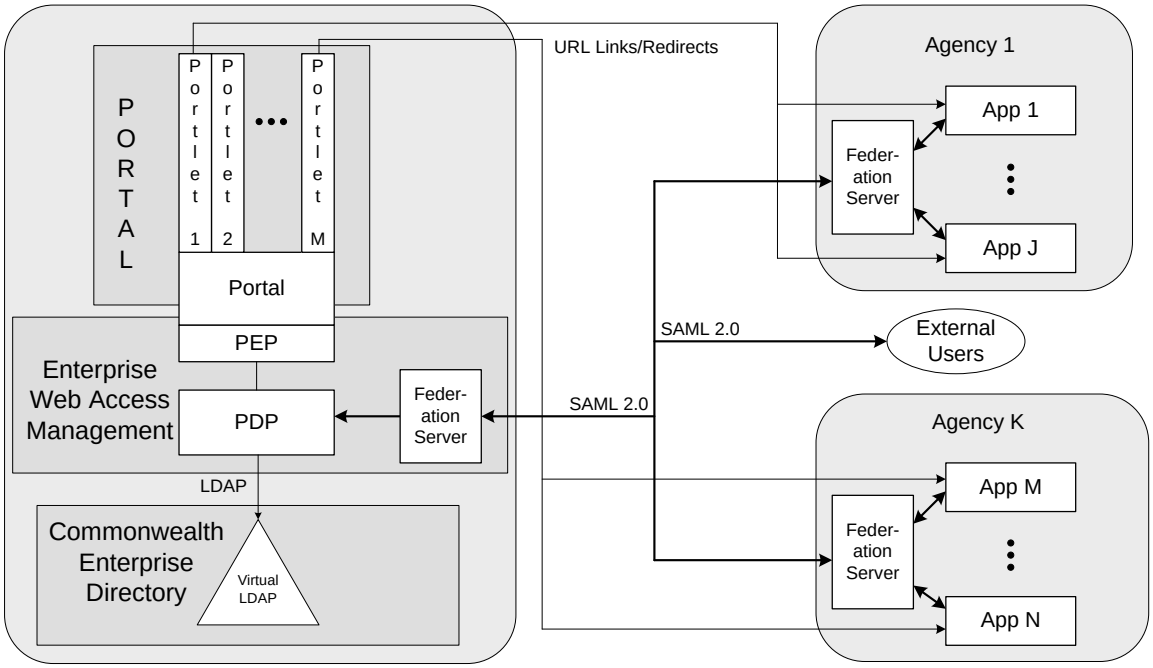

Figure 1 – Shared Authentication Service Architecture

This architecture is based on an EWAM system shown protecting the enterprise portal and using federation services (via the SAML 2.0 standard) to provide the user with access into the various agency sites.

Like most Web Access Managers, the EWAM protects Web-accessible resources based on policy. As shown, the EWAM is comprised of the following: a Policy Enforcement Point (PEP) that integrates with the Enterprise Portal to ensure that the required protection policy is enforced at the portal; a Policy Decision Point (PDP) that evaluates protection policies for one or more PEPs; an interface via Lightweight Directory Access Protocol (LDAP) to the Commonwealth of Pennsylvania Enterprise Directory (CoPED) to authenticate users and retrieve information about them; and a federation server to share authentication events to the agencies. These are discussed with additional details provided in the ensuing sections. A foundational use case for successful access is detailed in Section 5.3.

3.1 Enterprise Web Access Management

The Shared Authentication Service is provided via the Enterprise Web Access Management system (or Enterprise Web Access Manager, EWAM) as shown in Figure 1. These general systems provide centralized access policy management together with other features such as:

- A Web agent integrated with each Portal Server, serving as the Policy Enforcement Point (PEP) to interact with the user's communication stream to allow, block, or redirect access based on the defined policy;
- Two policy servers serving as redundant PDPs which:
    - Provide administration tools to define the policy

- Interact with the Policy Store to save and retrieve the policy
- Interact with the PEPs to make policy decisions on request
- Interact with CoPED to authenticate the user and to retrieve additional user information as required by the policy;

- Availability of multiple authentication methods, especially the ability to handle authentication for access to electronic resources using PIV smart cards as well as automated authentication for employees logged into their commonwealth Windows desktops;
- A Policy Store (database or directory) on each of the Policy Servers that stores the defined protection policy;
- Access to CoPED for user authentication and information retrieval;
- A built-in federation module that will receive SAML requests and issue SAML assertions to deliver authentication events to agencies and CoPs as trusted federation partners;
- Single Sign-On (SSO) allows a user to authenticate to the EWAM once and then be granted access to all applications and sites the user is authorized for. This service is to be provided within the Enterprise Portal by the EWAM and across the commonwealth through the use of the federation technology.

These features are explained fully in Section 4, Web Access Management.

3.2 CoPED Interface

CoPED is discussed in detail in the supporting document GEN-SEC013B *Directory Services Architecture*. CoPED provides a virtual LDAP interface for access by the EWAM for authenticating users and retrieving information about them. Behind that virtual interface, CoPED provides access to employees in Commonwealth of Pennsylvania active directory forest (CWOPA) and other specified users in certain defined identity stores at specific agencies; this is shown in *Figure 2 – Initial CoPED Architecture*.

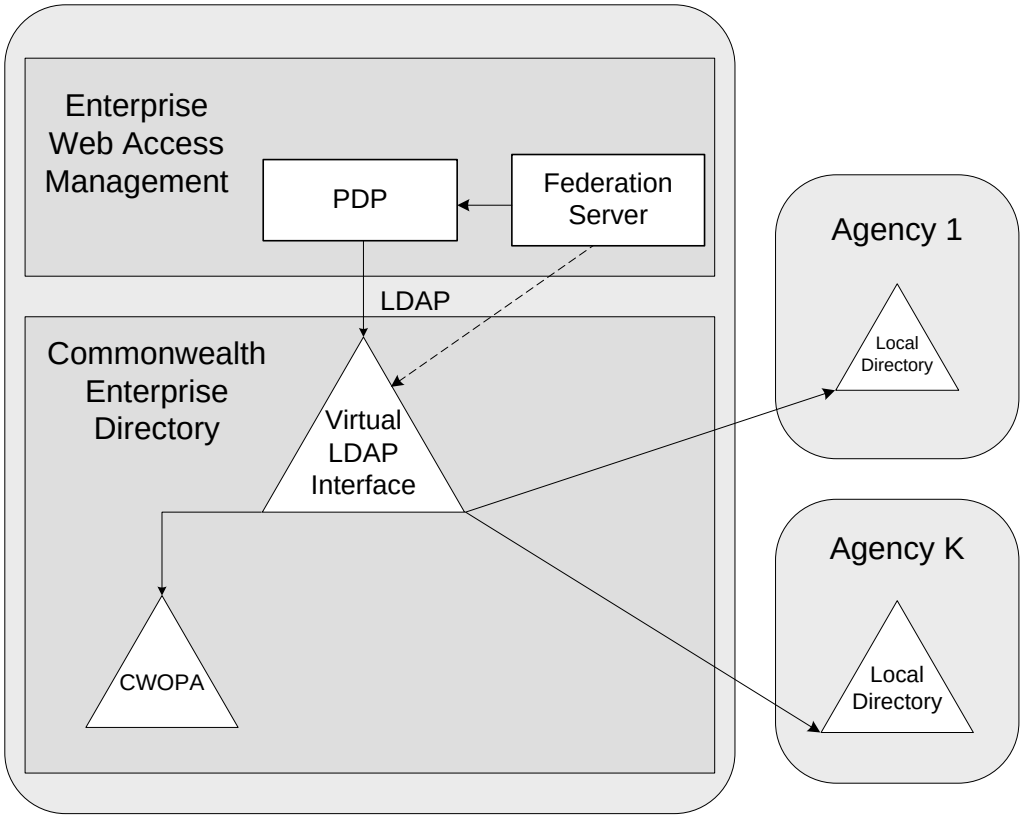

Figure 2 – Initial CoPED Architecture

CoPED is architected to evolve from this virtual representation of local identity data (excluding CWOPA for employees) into the actual domain directories: *Employee*, *Subscriber*, and *Business Partner* as described in GEN-SEC013B. This is illustrated in *Figure 3 – Final CoPED Architecture*.

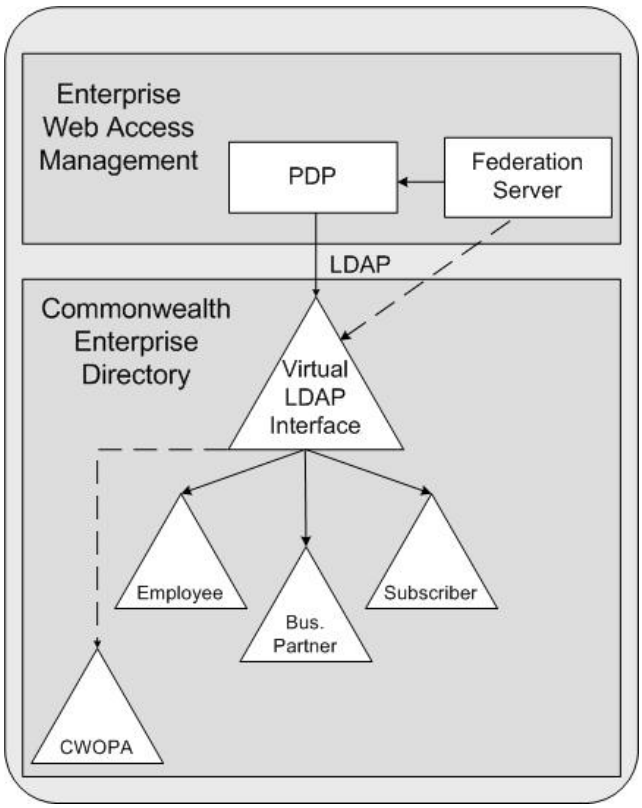

Figure 3 – Final CoPED Architecture

3.3 Federation

Federation allows disparate security domains to interoperate, and involves the creation of a trust relationship between the security domains. For any interaction the trust relationship defines two parties: the asserting party, also known as the Identity Provider (IDP), and the accepting party, known as the Relying Party (RP). Many industry standards for federation also refer to this party as a Service Provider (SP).

For the IPAM Shared Authentication Service, users authenticate to the EWAM when accessing the enterprise portal. When the user connects to an agency site from the portal, that site serves as the RP and requests an authentication assertion from the EWAM, which serves as the IDP. An assertion in this context is a claim regarding authentication, authorization, or attribute information applying to the user requesting access. The IDP makes assertions about the user's identity and the RP accepts those assertions. Section 5 provides a detailed description of federation.

3.4 Standards

The Shared Authentication Service is to follow all open standards listed in ITP-SEC013 as appropriate. In particular, the EWAM uses the LDAP v3 protocol to access the CoPED (whether for authentication or attribute gathering). The

Federated Single Sign-On uses the SAML v2.0 standard for requesting and asserting authentication claims, and is described in Section 5.

4. Web Access Management

The Shared Authentication Service is provided by a WAM system. These systems provide centralized access policy management together with many features such as multiple authentication schemes. The following sections detail the EWAM architecture, as well as provide additional guidance for agencies and CoPs implementing their own WAMs. These sections refer to Figure 4 – *WAM Web Agent Architecture.* STD-SEC014B - *Web Single Sign-on Standard,* names the commonwealth WAM standard.

4.1 Policy Enforcement Point (PEP)

Policy Enforcement Points (PEP) interact with the user's communication stream to allow, block, or redirect connections based on defined policy. For the EWAM, this is accomplished via Web Agent technology. A Web Agent is a software module that is installed on the Web server (could also be an application server if no Web server is used) to intercept the user communications before the Web server acts on them. These modules are customized for each type of Web server; for example, they are typically ISAPI filters for Microsoft Windows Internet Information Services servers or NSAPI filters for Sun Enterprise (or Netscape/iPlanet) Web servers.

The agent instructs the Web server to allow it to examine and evaluate each incoming message prior to the server's own processing. It will check for protection of the requested resource, current logged-in status of the user, and authorization of the logged-in user to access the resource, conversing with the PDP (or possibly a local cache) to perform its evaluations. The Web Agent will also gather user information returned from the PDP (as gathered from CoPED or the agency's local identity store) and pass it on to the Web or application server as cookie data or in the HTTP header of the page request. Finally, and regardless of whichever Web site is requested, the Web Agent makes a policy based redirect of the user to the

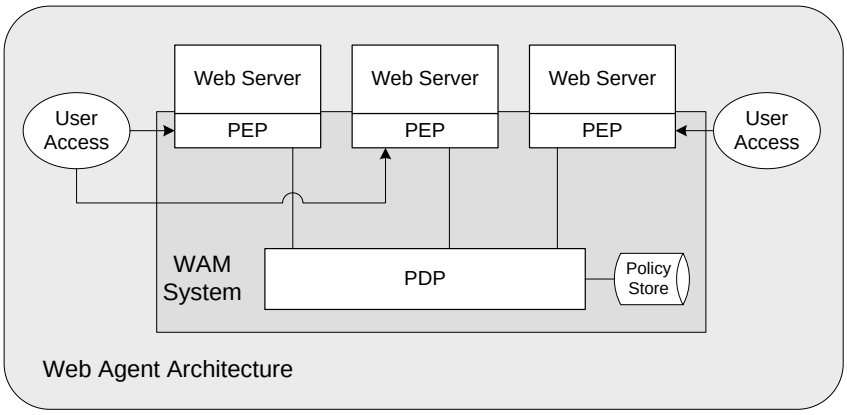

Figure 4 – WAM Web Agent Architecture

appropriate URL. This happens commonly when first authenticating to certain applications or portal environments, to be directed to a pre-defined start page, or to the next step in a work flow.

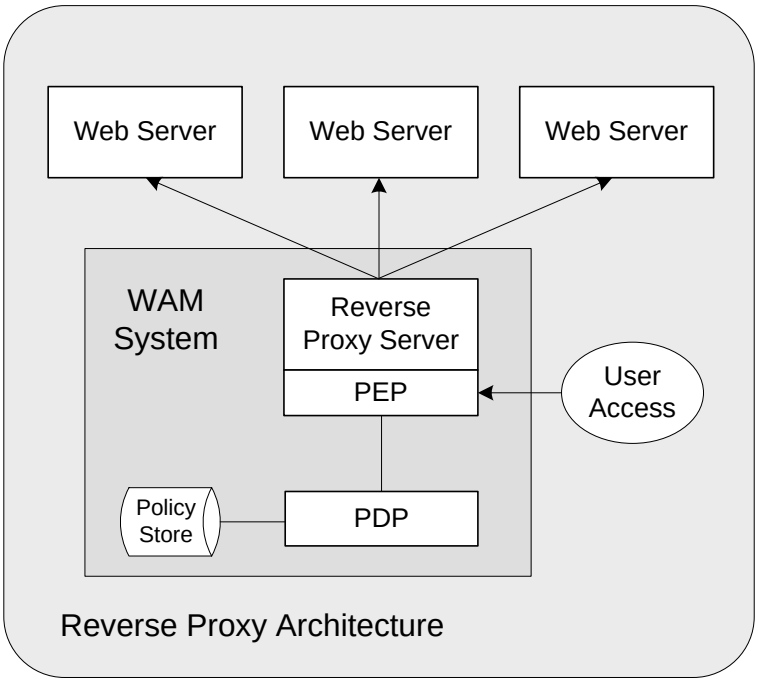

Figure 5 – WAM Reverse Proxy Architecture

In certain cases, an agency or CoP may decide to use Reverse Proxy technology for its PEP. A Reverse Proxy (sometimes referred to as a Secure Reverse Proxy or just Secure Proxy) is a separate server that is positioned between the users and the Web or application servers, and intercepts the user communications at that point. Other than this architectural difference, the Reverse Proxy operates essentially the same as the Web Agent. This might be useful for an agency or CoP that wants to protect several different brands of Web server (or where the set of platforms is in constant flux) that are co-located and have only a single access path for users to take. See *Figure 5 – WAM Reverse Proxy Architecture*.

4.2 Policy Decision Point (PDP)

The Policy Decision Point (PDP) is the central control point for the EWAM. It incorporates administrative tools to define and manage (e.g., backup) the protection policies defined for the commonwealth. The PDP interacts with the PEPs to make policy decisions in response to PEP requests, and typically interacts with the enterprise identity store (CoPED) to authenticate users and retrieve additional identity information according to policy requirements.

Although in practice multiple copies of the PDP often exist (i.e., multiple servers), these copies are to only exist when specific business needs require them. Reasons for providing multiple PDPs include:

- Failover – Most WAMs are inherently security systems. If the PEP cannot communicate with the PDP it assumes that it is under attack and will often

not allow further communications. It is therefore critical that the PEP be able to reach the PDP, so for any important Web site the corresponding PDP is to have a back-up PDP for failover.

- Load Balancing – For sites likely to be heavily loaded, the addition of redundant PDPs for load balancing can remove the PDP as a throttle point. Typically, a single redundant PDP can serve for both load balancing and failover.

- Geographic Distribution – If the security domain is distributed across separate physical locations, it is generally recommended (unless there is very high speed/bandwidth connectivity between the sites) to provide a redundant PDP at each location to facilitate PDP-PEP communication. These PDPs are to also have local copies of the identity store as well. As explained in the previous *Failover* section, anything that restricts the communication between PEPs and PDPs can potentially cause the PEP to think it is under attack and shut down the Web site it is protecting.

The EWAM is to have redundant PDPs (two servers total) to provide both failover and load balancing. Since these servers are co-located with the PEPs and CoPED at the Enterprise Portal, additional PDP servers for geographic distribution are not required.

4.3 Policy and Identity Stores

The PDP provides the administrative tools to manage the policies, which it generally stores in a separate directory or database. For the EWAM, the policy data will not be extraordinarily voluminous, and so is to be stored in a directory on the PDP server.

In addition to writing new or modified policy data to the policy store, the PDP also needs to access user data. For the IPAM EWAM, all users can be accessed via LDAP to the CoPED as shown in *Figure 2 – Initial CoPED Architecture* and *Figure 3 – Final CoPED Architecture* above. GEN-SEC013B describes the Enterprise Directory in detail.

4.4 Federation

A federation module is required, either as a component of the EWAM product or added on as a separate piece. The federation module requests, issues, and receives SAML requests and assertions to exchange authentication events with trusted federation partners. For the Shared Authentication Service defined in this document, the federation module is only expected to receive SAML requests from the agencies/CoPs and to issue SAML assertions back to them; any additional use of federation at the Enterprise Portal would require an approved modification to this document. Federation is detailed in Section *5 Federation*; the SAML assertion details are provided in Section 5.2.

4.5 Authentication Methods

The Shared Authentication Service is to provide, at a minimum, the four (4) authentication methods described below (i.e., x.509 certs, PIV card, User ID & Password, Windows Integrated).

4.5.1 X.509 Certificates

As part of a Public Key Infrastructure (PKI), users are provided one or more digital certificates. In particular, commonwealth users may be provided with a digital certificate defined to be used for authentication (i.e., with the *digitalSignature* bit set), either in a PIV card or independent of the card. Authenticating to the Shared Authentication Service using this certificate with a PIN will provide strong authentication.

4.5.2 PIV Card

There are several authentication methods that leverage the PIV cards and their respective assurance levels, primarily for physical access, which can also provide strong authentication. Authentication with the PIV card is explored in BPD-SEC013J - *Authentication via the PIV Card*.

4.5.3 UserID and Password

Until appropriate PIV cards are in widespread distribution (and probably for longer in the *Subscriber* namespace), many users will continue to leverage userID and password for EWAM managed applications that do not require very high Strengths of Authentication. ITP-SEC007 - *Minimum Standards for User IDs and Passwords* defines the commonwealth standard for the creation of passwords.

4.5.4 Windows Integrated

Employees who have logged into their commonwealth Windows desktop using their CWOPA credentials can be automatically authenticated by the EWAM leveraging the Active Directory Kerberos ticket and the use of Internet Information Services (IIS). Since contractors in CWOPA will not be authenticated by the EWAM against CWOPA, but rather the new *Business Partner* domain in CoPED, this functionality will not be initially available to them. Agencies are free to pursue this method of authentication when a high Strength of Authentication is not warranted (provided the EWAM is capable), or when that particular set of Windows desktops is well protected from rogue virtual private networks (VPNs) and wireless access points, or when additional authentication credentials in addition to passwords are utilized.

4.6 Authorization

Once the user has authenticated to the EWAM, the PEP then uses the defined policy to determine whether that user is authorized to access the requested resource. This policy is generally discussed separately between coarse- and fine-grained authorization. Coarse-grained (or just coarse) authorization refers to allowing a user to access a Web site or an application, whereas fine-grained authorization determines the detailed functionality available to a user once the application is accessed. Under the commonwealth's Core Shared Security Model, each agency

will retain control and execution of fine-grained authorization at its Web sites and applications.

The coarse authorization is to be shared between the EWAM, the Enterprise Portal, and the local agencies (either directly or by their local WAMs). The EWAM is to allow all authenticated users to access the Portal. Direct access to specific agencies or agency sites will be managed either directly by those sites or by that agency's own local WAM, which will presumably (although not necessarily) redirect the user to at least login through the portal (some sites will go further and redirect the user to a Portal-based "home" page, typically the AquaLogic My Page). The portal can allow access to various portlets based on roles specified in its internal repository via containers and groups in CoPED. All coarse authorization beyond that, including access to applications and sites requested via portal links rather than portlets, is to be managed by the agency sites or applications directly or by their own local WAMs.

4.6.1 Role-Based

One key factor in the authorization granted by the portal and the EWAM will be the user's role (or persona) as an *Employee*, *Business Partner*, or *Subscriber*, as many applications and sites will be restricted to one or two of these roles. Some additional role information may be generally available as well. For instance, entity files in the *Business Partner* domain will include an indication of the type of organization through which the user is a partner (county, municipality, non-employee first responder, contractor, federal, and other state), as well as the name of that organization; just as *Employee* entity files will include the hiring agency or department. When a user's authentication event is shared with an agency through federation, this role information is passed in the SAML assertion (see Section 5.2). The portal, working through the EWAM, is able to provide coarse role-based authorization according to these roles.

It is highly recommended that agencies base their authorizations (coarse and fine), at least initially, on user roles stored (statically or dynamically) in their local directories.

4.6.2 Rules and Conditions

In addition to the role-based authorization, both the EWAM and local agency WAM systems may use other rules, conditions, or business logic for access control. These rules are typically part of the protection policies that are implemented in the PDP for execution by the PEPs. For example, access might be dependent on:

- Time of day
- Access location
- Other attribute values besides roles

4.7 Single / Reduced Sign-On

One important benefit of the Shared Authentication Service is the ability to allow users to authenticate once and then have access to multiple commonwealth sites

and applications without being challenged again for credentials. This is commonly called Single Sign-On (SSO), and typically remains an unachieved goal. What is achievable is a lesser degree of SSO referred to as Reduced Sign-On (RSO), and is an expected feature of the Shared Authentication Service. The references to SSO below are indicative of the actual goal of true SSO, which is also a goal of the Shared Authentication Service, but pragmatically we may infer that what currently exists is a degree of RSO.

The Shared Authentication Service provides for SSO across commonwealth applications and sites by using federation (really only federated authentication). The SSO technology standard is named in STD-SEC014B - *Web Single Sign-on Standard.* The basic operation, as described in Section 5, allows a user to log in at the portal and gain access to all authorized applications and sites in the commonwealth enterprise without further challenge, with certain defined restrictions as outlined in the subsections below. This federation architecture provides the users with effective SSO without requiring the agencies to install tightly coupled, identical (or even similar) WAM systems; it only requires agencies to support the open standard for authentication federation, SAML 2.0 from OASIS (the Organization for the Advancement of Structured Information Standards), either directly in their application infrastructure or through a local WAM that supports SAML 2.0.

Although the OASIS SAML specification provides for the capability to perform global logout across the enterprise, the architecture defined here does not implement that functionality. This is because if the global logout were implemented, then any logout from any site (such as a timeout from an application that was no longer being used) would log the user out of all sites.

4.7.1 Single Namespace

SSO is only provided within a single domain; users who have personas (and corresponding accounts) in different domains will be challenged for credentials separately as *Employees*, *Business Partners*, and/or *Subscribers*. In most cases, for example, employees will also be subscribers (e.g., a school parent) and so will have two separate accounts for the two personas: *Employee* and *Subscriber*. Each persona will have its own credentials and its own set of authorized sites. SSO will be provided to the *Employee* account for all employee-related sites accessible through the portal; and to the school parent's *Subscriber* account for all education-related activities for the employee's child, as well as all other participating sites such as tax return data, welfare or mental health information, and vehicle and driver registration sites. But SSO will not span multiple domain accounts.

Similarly, many business partners will also be subscribers, especially municipal and county officials, and they will similarly have two separate accounts: *Business Partner* and *Subscriber*. Again, SSO would only be provided for one account in one namespace, not between the different accounts.

4.7.2 Identity Proofing

The WAM solution is used to pass the user's identity Assurance Level. The identity Assurance Levels are described in the supporting document GEN-SEC013D - *Enrollment, Identity Proofing and Vetting*, and define the security and depth of the process of vetting the user's identity prior to issuing the credentials. Certain sites will use this Assurance Level for determining whether to authorize access for a given user.

Unlike Strength of Authentication, if a user doesn't meet the required Assurance Level, that user cannot merely re-authenticate with a stronger credential. The agency that required that level will typically have the user redirected to begin that agency's vetting process to gain the higher level required for this site. In most cases the vetting will not be performed at that moment, and the practical effect will be to prevent immediate access to that site.

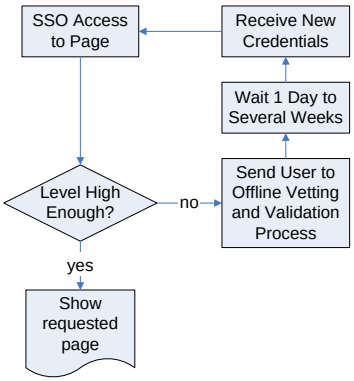

Figure 6 – Assurance Level Process Flow

4.7.3 Timeouts

It is a Web service best practice that all log-ins expire or "timeout" after a period of inactivity. Inactivity is an indicator that the client system may be unattended and exposes a security violation risk. All commonwealth secure Web sites are to incorporate timeouts. The logic is included in the commonwealth's EWAM solution. The timeout standard for a secure commonwealth Web page is twenty minutes. Total session timeouts are not to exceed eight hours. Timed-out users are to re-authenticate before resuming their sessions.

It is important to note that inactivity is measured as the time between submissions to the Web server. Activity at the desktop (such as data entry into a form) does not register until the page is submitted. Sites containing forms to be completed by the user that are long or complex may need to be broken down into multiple pages to prevent early timeouts for the user. Exceptions to the twenty minute standard will need to be approved via the regular exception waiver process.

4.8 Portal Integration

CoPA has standardized on the BEA AquaLogic Portal (formerly the Plumtree Portal), both for the centralized Enterprise Server Farm (ESF) as well as the agencies. The

Shared Authentication Service is to be provided by integrating the EWAM's Policy Enforcement Point (i.e., Proxy Server) with the front-end access to the Portal.

Detailed back-end access will be provided by federation of the front-end authentication to the local agency's SAML Federation Service, which can authenticate the user directly to applications or to a local WAM protecting the various applications and sites.

5. Federation

Federation allows disparate security domains to interoperate. Security domains that could not normally work together using applications that require identity information can work together using identity federation. Federation makes it unnecessary to force the consolidation of access management.

5.1 Overview

Federation involves the creation of a trust relationship between security domains. For an interaction the trust relationship defines two parties: the asserting party and the accepting party. The asserting party is also known as the Identity Provider (IDP); the accepting party is known as the Relying Party (RP). Many of the standards also refer to this party as a Service Provider (SP). The IDP makes assertions about the identity and the RP accepts those assertions. An assertion in this context is a claim regarding authentication, authorization, or attribute information applying to a subject for a specified resource.

In order for the necessary interactions to take place there is usually a federation service on each security domain. Although these services are to use the same standards to interoperate, it is not necessary for them to use the same products. It is also usually necessary to deploy proxies in front of or agents on the Web servers (or application servers) participating in federation (see Section 4.1 for a discussion of Web Agents and Reverse Proxies).

A simplified view of the process is depicted in *Figure 7 – Generic Federation Process Flow*. Keep in mind that the details, such as the use of cookies or the display of the IDP list, will depend on the agency's requirements, the product it selects, and its configuration and integration with the underlying applications. The flowchart is provided for architectural understanding only and is not to be construed as an actual design.

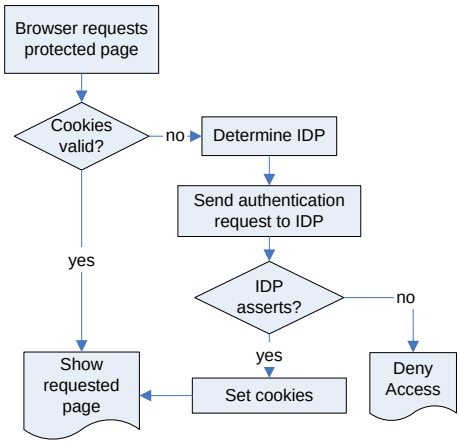

Figure 7 – Generic Federation Process Flow

Federation allows for Web Single Sign-On across separate but participating security domains. In federated environments, it is not necessary for each security domain to keep all of the user information for all of the participating security domains.

Instead, reliance on trusted IDPs allows users to access RPs that participate in the federated environment without being challenged for additional authentication.

5.2 Federation Process

The process of federation begins with authentication. The federation authentication domain (often referred to as a circle of trust) for the commonwealth, includes the EWAM as the IDP. Each of the agencies and CoPs acts as RPs. This provides a secure and seamless environment for users to transact business in. Although the existing legal relationships among the agencies are to be sufficient and preclude the need for any additional contractual or operational agreements, any agencies that want to leverage their federation infrastructure to provide access to users authenticating via outside IDPs are to establish appropriate business relationships with those IDPs, including contractual, architectural, and operational agreements.

Federated authentication for the Shared Authentication Service is to use the OASIS (Organization for the Advancement of Structured Information Standards) standard SAML version 2.0 for the necessary assertions between the IDP and the RP. These SAML assertions shown below in *Figure 8 – SAML Response Block*, are to occur over the Hyper-Text Transfer Protocol (HTTP) using the Simple Object Access Protocol (SOAP). There can be many additional parts and methods to the federation management environments; these options may be exploited by the agencies but are not required.

The SAML assertion issued in response to a SAML request from an agency or CoP

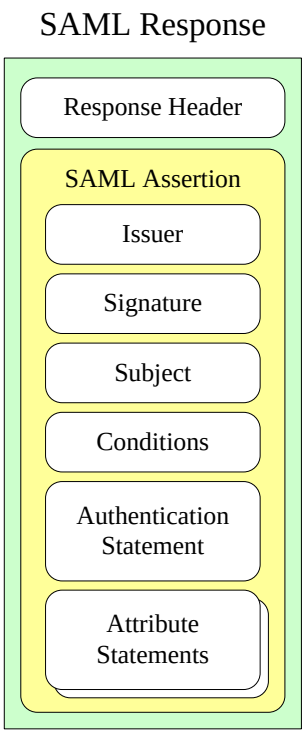

Figure 8 – SAML Response Block

identifies the user via the CoPED Global Unique ID (the CoPED GUID) attribute. The Attribute Statements will include other identifying information that may be useful to the agency's application, but the CoPED GUID is required for applications and sites accessed through the Shared Authentication Service unless the agency's local user ID is included in the information synchronized to CoPED. In either case, the identity information is to have been synchronized between the local identity store and CoPED for the connection to exist; see the supporting document, GEN-SEC013B. At a minimum this information is to include:

- Assurance Level for this account
- Agency that vetted the user
- Employee ID (if one exists)
- State-issued ID (driver's License number or non-driver's equivalent, if one exists)
- Associated ID (if one exists); for example:
    - If a user has been flagged for using fraudulent IDs and this CoPED GUID is one of those fraudulent IDs, the associated ID value would be the user's actual CoPED GUID.
    - If a user somehow ended up with two accounts and this CoPED GUID is one of the duplicates, the associated ID value would be the user's other CoPED GUID.
    - A tag will be included to indicate the reason for the associated ID.

5.3 Federated SSO Use Case

The Shared Authentication Service provides SSO across commonwealth applications and sites by using federated authentication. The basic use case operation is described as follows for the simple case where the user successfully authenticates and is authorized to access each page/application/site requested. In this description, each reference to an agency could also refer to a Community of Practice. See *Figure 9 – Shared Authentication Service Federation Architecture* .

1. User accesses the portal and is challenged for credentials by the PEP (i.e., the Proxy Server). The particular credentials requested will depend on the location accessed (username/password for low assurance sites, PIV or digital certificates for higher authentication strengths) and the EWAM policy implemented for that site.
2. User provides requested credentials to the PEP, which converses with the PDP to determine:

a. Is the user authentic (will typically include a conversation by the PDP with the CoPED to validate credentials, unless the user information is recently cached by the PDP)?

b. If yes, does this user have authorization to access the Portal?

c. If yes, should the user be redirected to a different URL? What URL?

d. If no, does this user have authorization to access the particular application or site that was requested in the initial URL?

e. What other information about the user is to be forwarded to the application or site? This will normally include the minimum authentication requirements and identity Assurance Level.

3. If the user selects (or is redirected to) a portal page (e.g., My Page), that page is displayed. If not, skip to step 5. In either case, the EWAM creates a session with the user's browser (typically by storing an encrypted, non-persistent cookie).

4. The user selects an application or site at an agency (via portlet or direct link). The Portal will direct the user's browser to the appropriate agency site.

5. The agency's local WAM checks whether the user has authenticated to it. Since the user has not, the WAM requests its local federation service to contact the enterprise WAM federation server to determine whether the user has authenticated at the portal.

6. The local WAM Federation Service sends a SAML request to the EWAM Federation Server. The EWAM Federation Server gathers the appropriate user information (CoPED GUID; assurance level and other ID information as described in Section 5.2, and possibly also enterprise-wide roles) and returns a SAML assertion claiming that the user has been authenticated to the defined strength.

7. The local WAM Federation Service then informs the WAM that the user is authenticated, and the WAM collects any other information it needs about the user from its local directories, based on the CoPED GUID or other ID returned from the enterprise, and creates its own session with the user's browser.

8. The local WAM, using all the information at hand, determines whether the user is authorized to perform the requested action.

9. If authorized, the user is then allowed to proceed using the requested application or site.

5.4 Mandated vs. Allowed

The architecture described in this document provides SSO across the commonwealth enterprise through the use of federation rather than mandating that

all agencies participate in a single EWAM security domain using a single EWAM product. There may, however, be smaller agencies that would request to be part of the EWAM as an economy of scale rather than implementing their own WAM or custom federation service. Such agencies are directed to join a CoP to provide the necessary scale.

5.5 Unique vs. Group Identity (Identity Mapping)

The federated authentication SAML assertion (shown connecting the federation servers in *Figure 9 – Shared Authentication Service Federation Architecture*) includes several attributes, most particularly the Global Unique ID (GUID) which uniquely and persistently defines the user across all domains and namespaces. For applications and sites accessed through the Shared Authentication Service, it is this GUID that links each user to his or her corresponding CoPED identity unless they have included their own ID for that user in the information synchronized to CoPED. In either case, the identity information is to have been synchronized between the local identity store and CoPED for the connection to exist; see the supporting document, GEN-SEC013B.

If an agency federates with organizations external to the commonwealth, however, it may choose to map the incoming users either to unique identities in its internal identity store, or to a single shared user (also known as a "group" user). This option is acceptable and appropriate when the access required is identical for each user, and there is no need to track which user accessed the application or site. For example, if the Department of Health wanted to post read-only health advisories

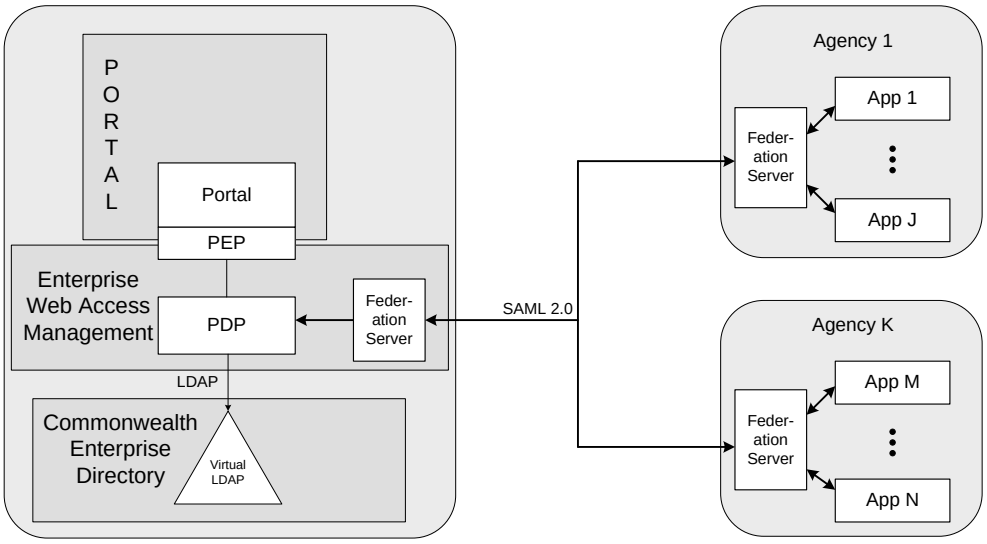

Figure 9 – Shared Authentication Service Federation Architecture

that were only accessible by county health officials, they may choose to create a site that used a group identity. In this case, a user would first authenticate to his county's main login page and then navigate to the DOH information site. The user is able to access the DOH site because the county's federation server sends a SAML assertion to the DOH site that the user had successfully authenticated with the role "County Health Officer." Agencies are free to establish separate groups for each defined role.

6. Governance and Administration

Ongoing governance for suggested modifications to the Shared Authentication Service will be provided by the IPAM Architecture Team rather than a separate dedicated organization, with the review and approval of the Bureau of Enterprise Architecture Standards Committee (EASC). Modifications approved by the EASC, including new functionality or integrations, are to be designed and implemented by a designated administrative group, the same group that performs the day-to-day operational oversight and management of the Shared Authentication Service.

Each agency specifies to this administrative group the coarse-grained authorization policy that will be required for each application or site. The two groups will work together to determine the appropriate split between the enterprise and local WAM systems for implementation of that policy. The IPAM Architecture Team is the designated arbitrator for all cases where an appropriate split cannot be agreed upon. Once a split is agreed upon, the designated administrative group will design, implement, and test the appropriate WAM policy to execute the agreed authorization policy.

Under the commonwealth's Core Security Model, each agency will retain control and execution of fine-grained authorization at its own Web sites and applications.

7. Federal Interoperability

Individual agencies are responsible for determining which Authentication Levels are required for access to their various physical and logical assets, according to their specific business and security needs. Higher Authentication Levels require a greater assurance that the user is who he claims to be. The Commonwealth of PA has established four Assurance Levels, and the minimum proofing requirements that are to be performed to achieve those levels. These are described in GEN-SEC013D.

Agencies seeking interoperability with federal or other related programs at a national level are directed to reference Federal Information Processing Standard 201 (FIPS 201), all National Institute of Standards and Technology (NIST) publications for federal interoperability, and Federal Bridge Cross-Certification publications. These publications establish a set of Authentication Levels and corresponding Assurance Levels that federal employees are to be vetted to before their Authentication Level is granted. The commonwealth named Assurance Levels that were explicitly constructed to conform to the federal Assurance Level standards. BPD-SEC013I - *Federal ID Assurance Standards* explains these relationships, and discusses the federal process for determining appropriate authentication mechanisms based on a standardized threat level assessment. Commonwealth policy for conducting threat level assessments is described in ITP-SEC005.

8. Related ITPs/Other References

- ITP-SEC013 - Identity Protection and Access Management (IPAM) Architectural Standard- Identity Management Services.
- APP-SEC013A - Identity Protection and Access Management Glossary
- GEN-SEC013B - Directory Services Architecture
- GEN-SEC013D - Enrollment, Identity Proofing and Vetting
- GEN-SEC013E - Specification for a Commonwealth Personal Identity Verification Card
- BPD-SEC013I - Federal ID Assurance Standards
- BPD-SEC013J - Authentication via the PIV Card.
- Federal Information Processing Standard 201
- ITP-SEC005 - Commonwealth Application Certification and Accreditation
- STD-SEC014B - Web Single Sign-on Standard

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	9/7/2006	Base Policy
Revision	9/25/2009	Updated format
	4/2/2014	ITP Reformat