COMMONWEALTH OF PENNSYLVANIA
DEPARTMENT OF PUBLIC WELFARE

INFORMATION TECHNOLOGY STANDARD

Name Of Standard: **Services Security**	Number: **STD-ENSS032**
Domain: **Security**	Category:
Date Issued: **09/07/2012**	Issued By Direction Of: Shirley A. Monroe Shirley Monroe, Dir of Div of Tech Engineering
Date Revised: **02/05/2014**	

Abstract:

This standard describes the Department's minimum expectations to secure "services" within the DPW Information Technology environment.

The following categories of services are defined based on service usage within the Department's infrastructure:

- **Enterprise Services:** A service developed for consumption by more than one application is considered an enterprise service. Enterprise services will be hosted in the Department's Service Oriented Architecture (SOA) environment and protected by the Department's standard services security product, "SOA Software Gateway".
- **Application Specific Services:** A service developed for consumption by a single application, which will not be reused by any other application, is considered an application specific service. Application specific services will be hosted in the Department's SOA environment and protected using the Department's standard services security product, "SOA Software Gateway".

Both enterprise and application specific services shall be virtualized and protected by the SOA Software Gateway which acts as a proxy to the back-end server. There shall be no direct access to consume services over the network. This rule may be waived if the client consuming the service and the service itself reside on the same physical server, and the service is bound to listen only on a non-routable interface (localhost or a named pipe).

Based on the service accessibility, the services can be deployed as:

- **Intranet facing service:** Source and the destination (server hosting the service) should be within the Department's infrastructure. Enterprise services, hosted on the Department's SOA infrastructure, should be deployed as an intranet facing service only. This service should not be exposed or accessed directly from the Internet.
- **Internet facing service:** Services that are developed for consumption directly (or through an application) by an Internet facing user are considered internet facing services.

Application development teams should try to re-use existing enterprise services before designing or developing an application specific service. This standard serves as a guideline for application development teams to select appropriate security controls to protect the services. The application development team must present the justification for the design of a particular service and associated security controls during the Architecture Review Board (ARB) sessions two and three. Usage of new application specific services must be discussed and approved during the ARB sessions.

The minimum security controls for protecting the services are discussed below.

General:

Services Security Standard applies to the Department of Public Welfare ("Department") services (defined in the following section) developed by the Department. The requirements outlined in this document are the minimum required to be considered adequate for securing the services for custom application development for the Department.

Standard:

During the Detailed Systems Design phase of Systems Development Lifecycle (SDLC), the application development teams should design at a minimum, the following security controls.

User groups consuming the service: The user groups who consume the services in the DPW infrastructure are broadly classified into

- Commonwealth users – Commonwealth staff and contractors
- Business partner users – Health and human service providers who have acknowledged the Commonwealth's Acceptable Use of Information Technology Resources (MD205.34)
- Citizen users – Pennsylvania residents applying for benefits using the Department's self-service benefits web applications such as COMPASS.

Service Modes: Service mode defines the type of service that can be developed. Services can be developed in one of the following service modes:

- **Web service**: Services that use the Simple Object Access Protocol (SOAP) messaging on Hypertext Transfer Protocol (HTTP) are considered web services. The communication channel between the source and the server hosting the web service should be encrypted using Secure Sockets Layer (SSL) v3 or Transport Layer Security (TLS) v1, with at least 128-bit key length. Web services shall be virtualized on the SOA Software gateway and accessed through a secured endpoint on the gateway.
- **REST service**: REST services are the required standard used for mobile websites and mobile applications. The communication channel between the source and the server hosting the rest service should be encrypted using Secure Sockets Layer (SSL) v3 or Transport Layer Security (TLS) v1, with at least 128-bit key length. Rest services shall be virtualized on the SOA Software gateway and accessed through a secured endpoint on the gateway.
- **Net.TCP service:** Synchronous services that are developed using Microsoft's Windows communication foundation (WCF) and use the **Net.TCP** protocol for communication are considered net TCP services. These services should be deployed as a Microsoft Windows based intranet services only. **Net.TCP** services shall be virtualized on the SOA Software gateway and accessed through a secured endpoint on the gateway.
- **Microsoft Message queuing (MSMQ):** MSMQ is an asynchronous Microsoft Windows service based messaging protocol that allows applications running on separate servers/processes to communicate in a failsafe manner. MSMQ can be used as application specific or enterprise wide intranet based services.
- **Named pipes:** Named pipes can be used to provide communication between processes on the same computer.

Authentication and authorization: The following security controls should be considered for providing user authentication and authentication to the service:

- The Department's standard tool, SOA Software Gateway should be used to protect web services.
- Authentication shall be performed based on user's Commonwealth credentials or Commonwealth service account and against Commonwealth standard directories.
- Individual user IDs should be used for authentication and authorization for internet facing services.
- Individual user IDs or Commonwealth service account should be used for authentication and authorization for intranet facing services.
- Standard security / authentication mechanisms include:

  - IP filtering (authenticating the request based on the client IP address)
  - Basic HTTP authentication
  - WS-Security with username and password digest
  - Mutual SSL authentication (with client certificate)
  - Two Factor Authentication (Client certificate and username/password)
  - Kerberos/Windows authentication can be used for authentication and authorization by **Net.TCP** and MSMQ services.
- Enterprise services that use service accounts for authentication and authorization should continue to use the service account provided to the respective consuming application. Service accounts must not be shared between applications. The same service account must not be used for production and non-production environments.
- Certificate based mutual SSL authentication or Two Factor authentication should be used for services interfacing with external entities like other Commonwealth agencies, CMS.

Communication security: The communication channel between the source and the service endpoint should be encrypted using SSL v3 or TLS v1 using at least 128-bit key.

Audit Logging: The service audit logs should record at a minimum, the following data elements

- Source application or IP address (optional)
- Target service and method invoked
- Service account or user ID used
- Timestamp
- Primary record identifier read/updated (if applicable).

Data and input validation: all services must perform user input/data validation prior to processing the request.

Outgoing services: third-party services consumed by Department's applications are considered outgoing services. Such services, hosted by external entities like other Commonwealth agencies or CMS, may present certain security requirements as specified by the entity hosting the service. Any service consumed by a DPW application must meet the following minimum security criteria:

- The communication channel between the source and the service endpoint should be encrypted using SSL v3 or TLS v1 using at least 128-bit key.
- Username/password authentication and authorization have to be performed.

Additional security requirements may be implemented based on the criticality and risk of the data. When applicable the Department's standard services security product, "SOA Software Gateway" must be used to implement security requirements, e.g.: to store client certificates and initiate 2-way SSL communication.
Implementation of specific security requirements must be approved by the Departments' Chief Information Security Officer (CISO).

The service security requirements are summarized in the table below.

Service Mode (Protocol)	Description	Service Type	User group	Authentication	Authorization	Communication Security	Audit Logging	Other Considerations
HTTP	Web services accessed using HTTP(S)	Enterprise – Public services (Internet usage; service consuming application does not require end user authentication)	Citizen users, Business partners and Commonwealth users	• SOA Software Gateway • Authentication to the SOA server based on calling application's service account • Two factor user authentication using certificates and user credentials for internet facing enterprise services.	• Application user roles based authorization using SOA Software Gateway	HTTP over SSL/TLS (HTTPS)	• Source application or IP address (Optional) • Target service and method invoked • Service account or user ID used • Timestamp • Primary record identifier read/updated (if applicable).	• Hosting a web service on a non-traditional port should be approved by BIS • Enterprise web services should be hosted on the designated SOA servers provided by BIS • Service account used to invoke the service should be the corresponding account assigned to the calling (source) application • User input / data validation must be performed by each service Leverage SOA Software if multiple methods in a web service require various access permissions to multiple user roles.
		Enterprise – External (Internet usage; service consuming application requires end user authentication)	Citizen users, Business partners and Commonwealth users	• SOA Software Gateway • Authentication to the SOA server based on calling application's service account.	• Application user roles based authorization using SOA Software Gateway	HTTP over SSL/TLS (HTTPS)		
		Enterprise – Internal (Intranet usage; service consuming application requires end user authentication)	Commonwealth users	• SOA Software Gateway • Authentication to the SOA server based on calling application's service account.	• Application user roles based authorization using SOA Software Gateway	HTTP over SSL/TLS (HTTPS)		
		Application specific web service (Internet and intranet usage; service consuming application requires end user authentication)	Citizen users, Business partners and Commonwealth users	• SOA Software Gateway • Individual user authentication.	• Application user roles based authorization using SOA Software Gateway	HTTP over SSL/TLS (HTTPS)		
Net.TCP	Windows Services using TCP protocol	Intranet only (Service consuming application requires end user authentication)	Commonwealth users	• SOA Software Gateway • Use WCF Security demand attributes.	• Windows group membership • Use at least two user groups to differentiate between Read/Update privileges authorizing to different methods/functions in the same service • Custom code to authorize to non-default Active Directory (AD) of the authenticated user (i.e. authentication and authorization ADs are different).	• Microsoft Windows Communication Framework (WCF) Transport Security	• Source application or IP address (Optional) • Target service and method invoked • Service account or user ID used • Timestamp • Primary record identifier read/updated (if applicable).	• Up to five TCP ports will be allocated for each service to serve the multiple DPW environments. The request for allocation should be submitted to BIS • Custom code used to authorize user or service account to authorize with AD user roles should be reviewed and approved by BIS. • User input / data validation must be performed by each service
MSMQ	Windows Services accessed via MSMQ protocol to achieve asynchronous communication	Intranet only	Intranet (server to server) or Local Machine only	• Windows authentication • Use Security Demand Attributes.	• Windows group membership • Use at least two user groups to differentiate between Read/Update privileges authorizing to different methods/functions in the same service • Custom code to authorize to non-default Active Directory (AD) of the authenticated user (i.e. authentication and authorization	• Microsoft Windows Domain Account (service account)	N/A (system event viewer/security event viewer logs)	• Windows permissions used to secure queues and to apply permissions for Read, Update and Delete operations

					ADs are different).			
Named Pipes	Intra-machine communication with Services achieved via Named pipes	Local machine usage only	Local machine usage only	N/A	N/A	N/A		N/A

Exemptions from this Standard:

Any exemptions to comply with this standard should be discussed with the Departments' Chief Information Security Officer (CISO).

Refresh Schedule:

All standards and referenced documentation identified in this standard will be subject for review and possible revision annually or upon request by the DPW Information Technology Standards Team.

Policy Supplements:

None

References:

1. Unified Security Standards for Web Applications (Version 1.2)

Standard Revision Log:

Change Date	Version	Change Description	Author and Organization
09/07/2012	1.0	Services Security	Clifton Van Scyoc
10/24/2013	1.1	Reviewed Content and formatted	Mathieu Saury
02/05/2014	1.2	Reviewed Content	Mathieu Saury