## 4.0 Security

System security was a primary consideration in the design of The Product and is integrated throughout the system. The Company security personnel used standard security features in the design to ensure only authorized users access the system and its data. The Product employs the following industry-standard security features:

- Secure Socket Layer connection for secure message transmission
- Lightweight Directory Access Protocol (LDAP) Directory service
- Page and field-level authorization
- Automated time-outs that automatically terminate unattended sessions
- Lock-outs for multiple invalid password attempts
- Single user multi-organizational support to allow a user to belong to multiple organizations, each having unique security privileges
- Data security provided through encryption to protect sensitive data during transmission
- Full audit-trail capabilities with the ability to track access to Protected Health Information (PHI)

The Product manages access to data through role-based security by allowing users to access system components and data appropriate to their user role and security profile. Users get several attempts to enter their password, after which, the system locks the user out and an administrator must then intervene. The Product also utilizes a keyed password feature that blocks the browser from recording passwords and provides audit trails using the user IDs.

The Product security features comply with the security requirements of A Federal Agency and align with the security and privacy principles of A Federal Technology Agency.

## 4.1 Security Architecture

The Product's system architecture is designed to meet the highest security standards. It employs strong technical controls and industry-standard security software to safeguard the system's data from threats and hazards and to restrict the availability of data to authorized users. Based on a Java Enterprise Edition (JEE) platform, the system uses a role-based security model that allows users to have appropriate access roles based on business need. Security software includes IBM Tivoli Identity Manager, IBM Tivoli Access Manager and WebSEAL, providing a comprehensive solution for managing identity profiles and permissions.

The Product's system architecture includes protection via the demilitarized zone (DMZ) and various network devices including intrusion detection systems, firewalls, and email filtering as depicted in Exhibit X.X.X, Security Architecture and Components. This architectural approach provides protection from access over unauthorized protocols, and from denial of service and other protocol-related attacks. Access to the DMZ is blocked by default within the firewalls and access lists on the Internet routers. Source hosts and networks, destination hosts, and specific protocols and ports are specified in firewall rules and router access control lists (ACL). Firewall and access list changes are performed regularly.

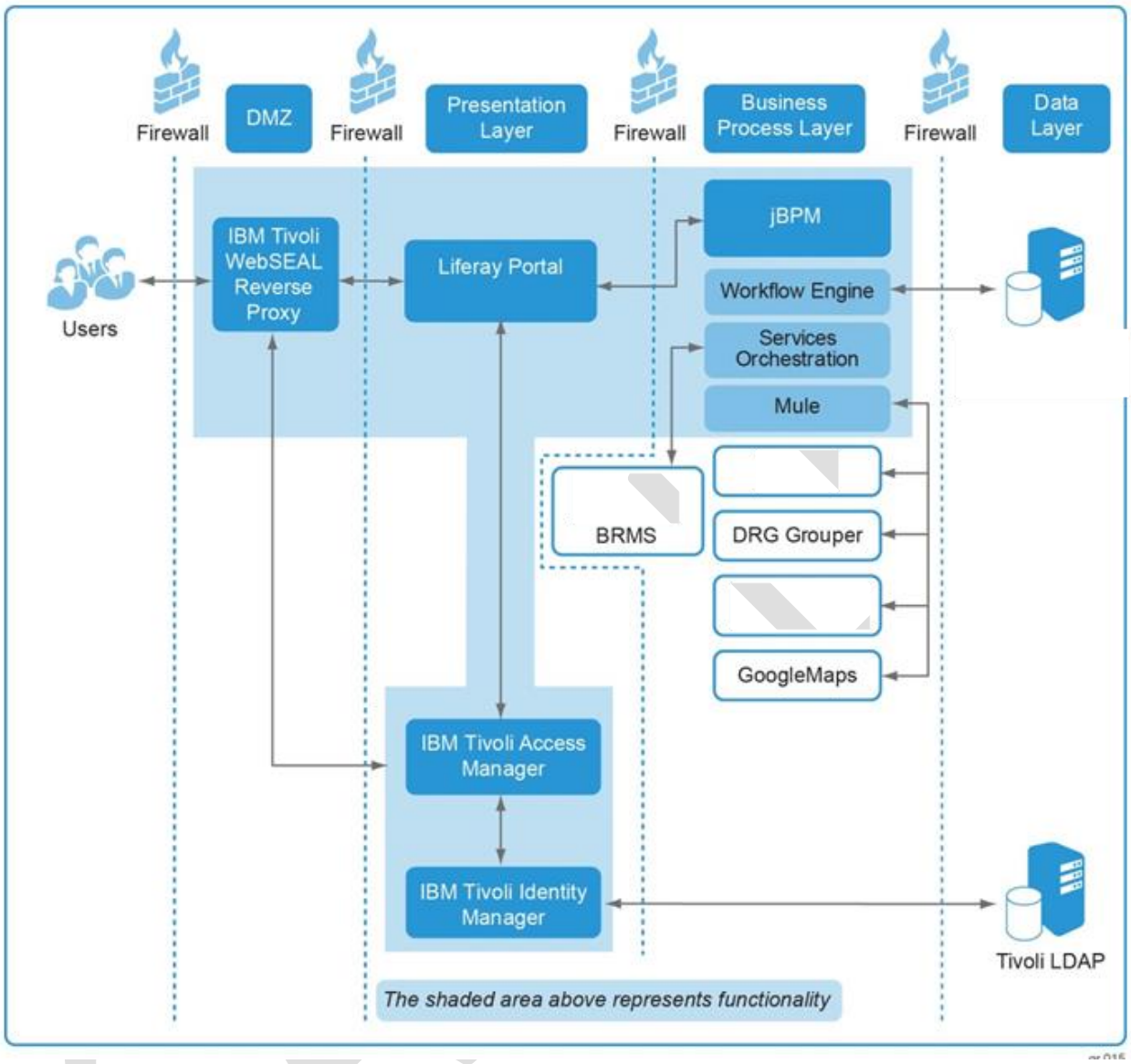


**Exhibit X.X.X. Security Architecture and Components**

*The Product utilizes three distinct firewalls to secure the system, application, and data.*

### 4.1.1. Firewall Protection

The Product's firewalls prevent unauthorized traffic into and out of the secure network. We use three firewalls, as depicted in Exhibit X-X, Firewall Protection:

- Domain (Internet) Firewall: Protects from unwanted intrusions directly from the internet. All The Product Internet Packets are routed through WebSEAL. This firewall resides in the DMZ. It protects against unwanted or undesirable information streams.

- Application Firewall: Protects all applications and the LDAP units where data is stored. This is the firewall that protects the internal application programs and some of the application repositories.

- Data Firewall: Protects The Product, COTS databases, and LDAP storage units. This firewall resides between the Portal and Oracle databases, protecting the databases and other application repositories.

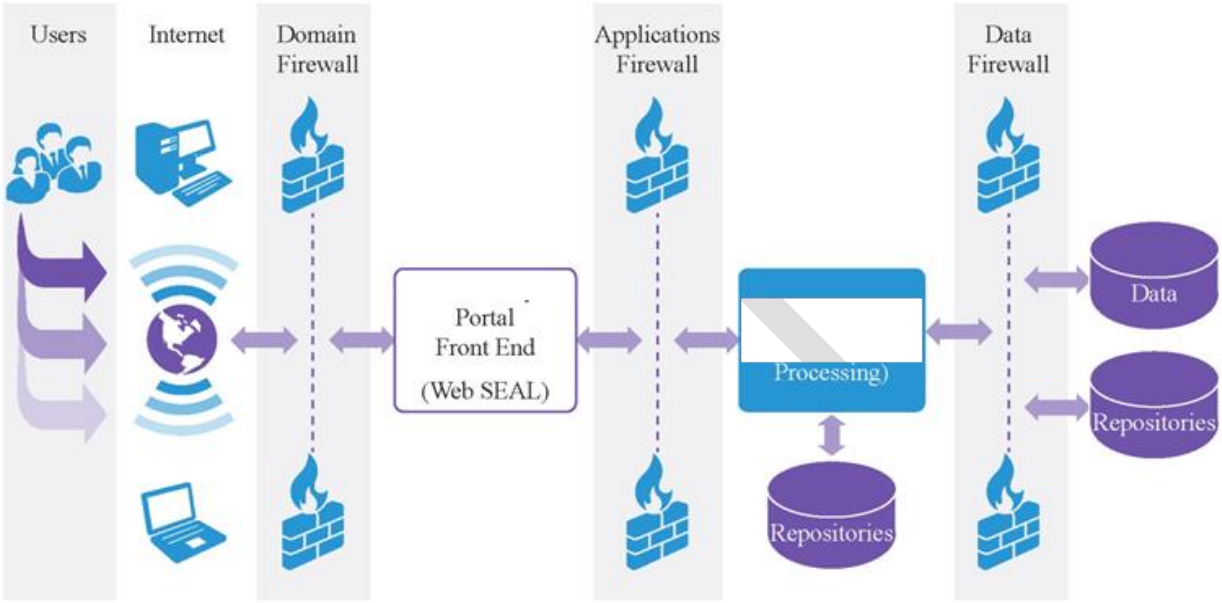


**Exhibit X-X. Firewall Protection**

*The Product utilizes three distinct firewalls to secure the system, application, and data.*

After the user accesses the Internet through the first network firewall (the domain firewall), there are front-end security entities that process secure user identification, authentication, authorization, and provisioning.

## 4.2 Security Tools

IBM Tivoli Security Suite is a comprehensive portfolio of security, risk, and compliance management tools for managing identity profiles and permissions for The Product's dynamic infrastructure. Table X.X.X, The Product Security Tools, provides a high-level description of the tools used for security.

| Table X.X.X, The Product Security Tools | |
|---|---|
| **Tool** | **Description** |
| **Secure Socket Layer (SSL) connection** | SSL uses the public-and-private key encryption system that includes a digital certificate. This protocol manages the security of message transmission and the passing of data back and forth between program layers in The Product. |
| **Hypertext Transfer Protocol Secure (HTTPS)** | The HTTPS protocol provides communications security over the Internet. HTTP is layered on top of the SSL/TLS protocol, providing additional security for The Product. HTTPS also provides bidirectional encryption of communications, protecting against malware, spying, eavesdropping, and tampering with communication content. |
| **External and Internal Demilitarized Zones (DMZs)** | A demilitarized zone is a configuration that includes multiple firewalls to add layers of protection. It is a boundary between public and private information that resides on a public domain, such as the Internet. The DMZs add an additional layer of security between the Internet and The Product's data. The Product uses two DMZs, external and internal, to ward off external attacks and to protect the data. |
| **Virus Protection** | Virus protection software prevents viruses, worms, Trojan horses, and the like from infecting computers. We use Symantec's Norton Antivirus. |
| **Firewalls** | A firewall is a network configuration that prevents unauthorized traffic into and out of a secure network. The Product uses two firewalls prior to users accessing the actual application:<br>• One in the DMZ after getting through HTTP<br>• An application firewall<br>The system uses a third firewall between the Portal and the Oracle databases. |
| **IBM Tivoli Security Suite** | The Product system uses Tivoli Identity Manager, Tivoli Access Manager, and Tivoli WebSEAL for authentication and provisioning and to protect the data and identities within the system. |
| **IBM Tivoli Identity Manager (TIM)** | TIM provides identity management and a centralized means of creating, deleting, and updating users within the system. It also provisions this information to target systems, such as Tivoli Identity Manager Agents. As part of the license, it includes:<br>• IBM Tivoli Directory Server: A Lightweight Directory Access Protocol (LDAP) for all users managed by both TIM and TAM. It provides the central repository for user data.<br>• IBM Tivoli Directory Integrator (TDI): Supports data synchronization between different data stores and supports different connectors and event handlers to monitor data changes or accepts data changes by listening in server mode. |
| **IBM Tivoli Access Manager (TAM)** | TAM provides role-based authentication and authorization definition to individual system resources and controls the behaviors that can be applied to or by those resources. |
| **IBM Tivoli WebSEAL** | WebSEAL is a secure reverse proxy that provides URL filtering and global sign-on to access the The Product system in the network layer. The reverse proxy server acts as a front-end authentication server and passes the HTTP/HTTPS request to the back-end servers. |

### 4.2.1 Identity Management

The Product performs identity management through architectural integration of the IBM Tivoli Security suite. The Product uses WebSEAL and TIM to provide identity management. TIM maintains the list of users who are permitted to access the system. It stores this information in the Lightweight Directory Access Protocol (LDAP) database and provides a centralized means of creating, deleting, and updating users within the system and provisioning this information to target systems.

### 4.2.2 Access Management

The Product uses SSL connections through HTTPS for communications with users' browsers. The only entry point from the public Internet into The Product is at the IBM Tivoli WebSEAL server. TAM and WebSEAL together provide role-based access to The Product Web pages, portlets, and other resources (An example of a resource is a portlet).

TAM provides role-based authentication and authorization definition to individuals and system resources and controls the behaviors that are allowed by those resources. Integrated with TAM, The Product enforces role-based security at the portlet level. It authenticates users against TAM and allows them access only to those parts of the portal for which they are authorized. When any user attempts to access The Product, WebSEAL authenticates the user credentials and passes them to the appropriate area.

The Product uses WebSEAL to apply its security policy to all users attempting to access portal resources. WebSEAL provides the gateway through which all portal access passes. WebSEAL is a high-performance, multi-threaded Web server that applies security policy as defined in TIM and TAM to all users attempting to access portal resources. It is used as a reverse proxy server. As such, it routes in-bound network traffic to portal and back-end services while presenting a single interface to the caller. The caller may be a browser or other applications. WebSEAL determines if the user has attempted to access a protected resource and prompts the user with a logon dialog. WebSEAL validates the identity of users through the LDAP directory and TAM. WebSEAL provides a first line of defense by separating or masquerading the type of server that is behind the reverse proxy. This configuration protects the portal and application servers through a process called obfuscation. Any rogue request is monitored and blocked by the security administrators using a Session Management server, which is integrated with WebSEAL.

Exhibit X.X.X, Security Architecture Tools, illustrates the interconnectivity of The Product's security tools.

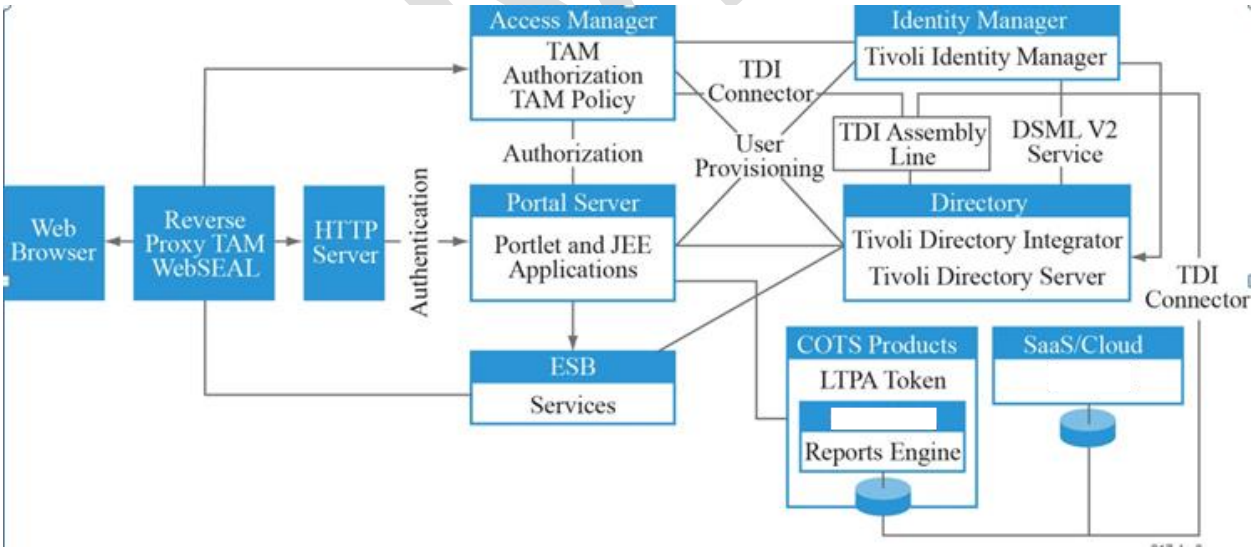


**Exhibit 4-2. Security Architecture Tools**

*The Product engages several tools to secure the system, application, and data.*

### 4.2.3 Single Sign On

The Product provides a single sign-on (SSO) point for all users, simplifying use and improving security by reducing the number of logins a user manages. Role-based authentication limits user access to only that data and those functions for which the user is approved, and 128-bit SSL encryption prevents hackers from "sniffing" the data in transit. Firewalls protect The Product from unauthorized access to the Web servers, and the tiered architecture imposes more firewall constraints on access to the application servers and database servers. We provide further protection through a Network Intrusion Detection System (NIDS) that monitors the network.

The Product uses WebSEAL and TAM to enable SSO with Liferay Portal and all of the integrated COTS products. The supported SSO mechanisms within WebSEAL include:

- Trust Association Interceptor (TAI)
- Light Weight Third Party Authentication (LTPA)
- HTTP Headers
- Global Sign on (GSO)
- Forms Based Authentication

WebSEAL provides global sign-on to access The Product in the network layer using Junctions. A WebSEAL junction is a TCP/IP connection between a front-end WebSEAL server and our Web-application server. Junctions are security pathways that direct authorized users to the appropriate parts of the system. Junctions between cooperating servers result in a protected, unified, distributed Web space that is seamless and transparent to users.

TAM allows users to log into multiple Product applications with a single password, streamlining user access with automated sign-on/sign-off, which simplifies security and management. This setup also facilitates regulatory compliance with fine-grained audit logs and enhances strong authentication choices.

Initial access to the The Product Web application is through our Web portal Home page. The single sign-on solution in The Product allows the user to access a resource, regardless of the resource's location, using only one initial login. Any further login requirements from portal applications are transparent to the user.

## 4.3 Role-Based Provisioning

The Product's provisioning process monitors access rights and privileges to ensure the security of The Product resources and users privacy. The Product uses TIM, the XXX Application Programming Interface (API), and Tivoli Director Integrator (TDI) to achieve role-based provisioning.

In our role-based provisioning model, when role changes are submitted to the The Product system by an authorized administrator, TIM evaluates its policy and provisions access to the required back-end resources and a user is only added to a back-end system when they have one or more of the appropriate roles. The Product stores user provisioning information in TIM, which captures the details from the screen and calls a service. There are multiple databases to which The Product sends the user information. TDI tells where the user information can go, such as to LDAP or Oracle. TIM automates the creation, modification, recertification, and termination of user privileges throughout the entire user lifecycle. Using TIM, The Product establishes formal processes for validating access, facilitates critical compliance requirements, mitigates risk, and enhances security by preventing user access conflicts.

The Product uses the XXX API to provide a provisioning platform for password, identity, and account management. The XXX API makes these management tasks easily extendable, yet keeps the system secure. For example, it makes it possible for users to safely change their passwords without accessing the Web console, which provides an added layer of security.

The Product transforms, moves, and synchronizes generic and identity data residing in heterogeneous directories, databases, files, and applications with real-time automated updates to the authoritative data source using TDI. TDI also helps enhance the security, accuracy, and integrity of generic and user identity data, while facilitating data migration, transformation to other file formats and synchronization between two or more components in The Product.

### 4.3.1 Role-Based Security

Role-based security limits user access to the minimum necessary data and those functions for which the user is approved. The Product manages role-based security using TAM, which stores pre-assigned roles and privileges (access controls) for each user and all data. A role is a configurable, defined group of privileges assigned to every user. Every role is assigned privileges (rules and procedures) that are specific to the role, and a role can have several privileges, and a privilege can be assigned to multiple roles as depicted in Exhibit X.X.X, Role-Based Security.

IMAGE REMOVED FOR SAMPLE

**Exhibit X.X.X, Role-Based Security**

*The Product's role-based model provides secure access to data, applications, and resources.*

The Product uses Liferay Portal configuration to grant authorization to specific items. SSO integration with TAM and WebSEAL enables Liferay portal to retrieve the logged-in user's role/privilege information. Each page in Liferay portal is associated with a list of roles and privileges that can access that particular page. Therefore, a user can only see the pages that their role assignments authorize them to view. When a portal page is requested, The Product performs checks to determine if the portal page is a protected resource and which roles have access to the portal page. If the user is authenticated and has the defined roles and privileges, the protected resource is displayed for the user. CONTENT REMOVED FOR SAMPLE.

CONTENT REMOVED FOR SAMPLE.

## 4.4 CONTENT REMOVED FOR SAMPLE

## 4.6 Summary

The The Product security infrastructure contains multiple layers of security that protects its users, data, applications, servers, and databases, while ensuring that access to The Product is tightly controlled and monitored. Our security framework includes tools and components that protect against malicious attacks, internal and external intrusions, and unauthorized access as depicted in Exhibit X.X.X, Interconnectivity of The Product Security Elements. We also engage numerous standard security features, such as multiple firewalls, virus protection, SSL, HTTPS, user authentication, and password encryption to ensure that The Product users, data, and resources are secure and protected.