Interface Requirements

Department of Veterans Affairs

Office of Information and Technology (OIT)

March 2022

Version 1.0

Revision History

Date	Version	Description	Author
03/31/2022	1.0	Initial Version	VistA Office

Table of Contents

Interface Requirements

1. Introduction

The purpose of the Interface Requirements section is to provide guidance to both Product owners and developers on the implementation of common Veterans Health Information Systems and Technology Architecture (VistA) interfaces that communicate and transmit data between two or more applications or systems. Following the tenets of the Identity Management process to ensure user account creation, proper permissions are applied, changed, or disabled according to standard practices, a keen focus on User Identity Provisioning, User Authentication, and User Authorization must be woven within interface development practices.

This document uses the terms Fundamental and Non-Fundamental Interface to describe interfaces that use standardized and non-standardized methods to connect an interface to VistA. Fundamental interfaces are interfaces that follow the practices outlined by both Kernel Security and Identity and Access Management Development teams respectively, while Non-Fundamental Interfaces use non-standard practices to connect to VistA. Through the lens of both fundamental and non-fundamental interfaces, the ultimate goal of the information in this section is to guide product line managers and developers to use standardized interface development practices to avoid the pitfalls that negatively impact the timely release of a product, which is almost always linked to a gap in security.

2. Process

This section encompasses the three primary methods all developers should follow when developing remote connections to applications or systems. Terminal Sessions via Secure Shell, Remote Procedure Calls, and VistA Link are the three primary remote connections that are used to connect an application or system within VistA. Throughout this document, the three primary remote connections are termed “fundamental interfaces” used within VistA. The term fundamental interface is used to identify the most common remote connection interfaces that has been well documented, developed, and follow a specific implementation standard in VistA. Project managers or developers should review the steps in each section to include following the links that further explain connection procedures. Additionally, there are non-fundamental interfaces such as VistA Integration Adapter, Server Options, MUMPS-to-MUMPS (Massachusetts General Hospital Utility Multi-Programming System) Server, and Veterans Data Integration and Federation (VDIF) architecture that are used by remote connections. The non-fundamental interfaces are unique remote connections that all follow a different documented, developed, and implementation process.

2.1. Fundamental Interfaces

Fundamental interfaces in this document refers to common authorized interfaces used within the VA system.

2.1.1. Terminal Secure Shell (SSH)

The Terminal via Secure Shell (SSH) interface provides the traditional VistA text-based interface that is driven by VistA Menu Management (MenuMan). The application Menu is assigned to each user as their primary menu. When the user accesses VistA through this interface, MenuMan displays the primary menu, along with the menu's child options for the user to choose from according to their role in the organization. The following are how users connect, receive authentication, and gain authorization to VistA through the approved Terminal Client application Micro Focus Reflections:

- User Authentication credentials are at the Local level in order of availability
- The IAM STS SAML token (SSOi) is obtained after user authenticates with IAM using the following methods:
  - User's PIV card certificate and private key PIN
  - VA Network username and temporary password
  - VistA Access and Verify codes
- Remote User Authentication credentials for Visitor are not available using Remote Terminal via Secure Shell
- User Authorization occurs through Vista Menu Manager
  - The user must have a Primary Menu Option assigned
  - The user must have the necessary Security Keys

2.1.2. Remote Procedure Call (RPC) Broker

The RPC Broker interface provides a Windows GUI environment. There are two separate components: VistA-side Broker; and a Delphi-based Broker client SDK. The application components are displayed on the GUI. Actions or events on the GUI are translated to remote procedures that are invoked in the VistA side. The application components are assigned to each user as one of their multiple secondary menu options (B-type). When the user accesses VistA through this interface, MenuMan is checked before the corresponding remote procedures are invoked. The result of the remote procedures is then displayed in the GUI components of the application. The following are how users connect to VistA using the Remote Procedure Call Brokers SDK:

- User Authentication credentials at the Local level following the order of availability below:
  - The IAM STS SAML token (SSOi) is obtained after user authenticates with IAM using the following methods:
  - User's PIV card certificate and private key PIN.

    - VA Network username and temporary password
    - VistA Access and Verify codes
- Remote User Authentication credentials (Visitor): It is critical that development teams register their remote connections with IAM as a Remote Application. The following are the steps by which remote authentication occurs:
    - IAM STS SAML token (SSOi), obtained after user authenticates with IAM using the following methods:
        - User’s PIV card certificate and private key PIN
        - VA Network username and temporary password
        - VistA Access and Verify codes
- User Authorization occurs through the Broker Security Menu Manager
    - The user must have at least one Secondary Menu Option assigned, and the Option must be B-Type
    - The user must have the necessary Security Keys

2.1.3. VistA Link

VistA Link: The fundamental interfaces of VistA Link, Remote Procedure Calls, and Terminal provides a Web based GUI environment. There are two separate components: VistA-side Broker-like component; and a Java EE Application Server client SDK (VistALink Connector). The application components are displayed on the Browser. Actions or events on the Browser are translated to remote procedures that are invoked in the VistA side. The application components are assigned to each user as one of their multiple secondary menu options (B-type). When the user accesses VistA through this interface, MenuMan is checked before the corresponding remote procedures are invoked. The result of the remote procedures is then displayed in the GUI components of the application. Note that VistALink applications also make use of security keys that are translated to Java EE Groups, which are then used to protect web page URLs. The approved VistALink Client application is WebLogic Java VistALink Connector which prompts for the approved credentials.

- User Authentication credentials at the Local level follow the order of availability below:
    - Identity and Access Management (IAM) Security Token Service (STS), Security Assertion Markup Language (SAML) token, Single Sign-On internal (SSOi), obtained after user authenticates with IAM using the following methods:
        - PIV card certificate and private key PIN
        - VA Network username and temporary password
        - VistA Access and Verify codes
- Remote User Authentication credentials (Visitor): It is critical that development teams register their remote connections with IAM as a Remote Application. The following are the steps by which remote authentication occurs:

    - IAM STS SAML token (SSOi), obtained after user authenticates with IAM using User's
        - PIV card certificate and private key PIN
        - VA Network username and temporary password
        - VistA Access and Verify codes
- User Authorization occurs through the Broker Security Menu Manager
    - The user must have at least one Secondary Menu Option assigned, and the Option must be B-Type
    - The user must have the necessary Security Keys

2.2. Non-fundamental Interfaces

Non-fundamental interfaces provide a process and setup like Fundamental Interfaces such as VistALink but with significant differences that are documented here. There are several components, but these can be generalized as two components:

- VistA-side APIs for Authentication and Authorization; and
- an InterSystems Web, REST, or SOAP application.

The application components are exposed as Web APIs (as Endpoints) to be consumed by other systems using an HTTP(S) client. Incoming HTTP requests directed to the Endpoints are translated to invocation of existing routines or FileMan access or Global access on the VistA side. The set of Endpoints are assigned to each user as one of their multiple secondary menu options (B-type). When the user accesses VistA through this interface, MenuMan is checked before the corresponding VistA resources are accessed. The result of the VistA access is then returned in the payload of the response, corresponding to a Web, REST, or SOAP response. VDIF is an example of such interface; there have been other interfaces in the past, like Beneficiary Travel, and new ones may be developed in the future.

2.3. Veterans Data Integration and Federation (VDIF)

The VDIF client-side connection is an InterSystems Web, REST, or SOAP application; The VistA side of the connection is a direct access to the corresponding VistA namespace. VDIF connections can access any of the VistA systems through an Enterprise Cache Protocol (ECP) connection.

- User Authentication credentials at the Local level following the order of availability below:
    - IAM STS SAML token (SSOi), obtained after user authenticates with IAM using the following methods:
        - PIV card certificate and private key PIN; or
        - VA Network username and temporary password
        - VistA Access and Verify Codes
- Remote User Authentication credentials (Visitor): It is critical that development teams register their remote connections with IAM and the VistA Office as an approved Remote Application. The following are the steps remote authentication occurs:

    - IAM STS SAML token (SSOi), obtained after user authenticates with IAM using User's
        - PIV card certificate and private key PIN; or
        - VA Network username and temporary password
- User Authorization occurs through the Broker Security Menu Manager
    - User must have at least one Secondary Menu Option assigned, and option must be B-Type that contains a list of named Web Endpoints
    - User must have the necessary Security Keys

Following the Interface requirements guidance, all product and development teams will properly register their interfaces and follow the standards of developing remote applications and interfaces to ensure Zero Trust on the Enterprise VistA System.

3. References

The following reference documents are available at this link:

https://dvagov.sharepoint.com/sites/OITEPMOVistAOffice/Shared%20Documents/Forms/AllItems.aspx?csf=1&web=1&e=fBBcZk&cid=03abded4%2D7fe1%2D4fdb%2D80c9%2D0b1c8d2c3997&RootFolder=%2Fsites%2FOITEPMOVistAOffice%2FShared%20Documents%2FVistA%20Guide%2FInterface%20Requirements&FolderCTID=0x012000A78B13F55919A445A6B2436281DF8EA8

- Interface Requirements Version 1.0
- VistALink System Management Guide Version 1.6
- VistALink Developer Guide v 1.6
- Kernel Authentication & Authorization for J2EE – KAAJEE
- RPC Broker 1.1 Developer Guide.
- FileMan Delphi Components 1.0 (FMDC) Getting Started Guide,
- FileMan Delphi Components (FMDC) Technical Manual and Security Guide
- Kernel 8.0 & Kernel Toolkit 7.3 Developer's Guide
- VistA Health Level Seven (HL7) Site Manager and Developer Manual
- Health Level Seven Optimized (HLO) Developer Manual
- HealtheVet Web Services Client (HWSC) 1.0 Developer's Guide

4. Contact

For more information on Interface Requirements, please contact the VistA Process Governance Workgroup at VISTAProcessGovernanceWorkgroup@va.gov