Electronic Signature (ESig)
Version 1.0

Installation Guide

November 2006

U.S. Department of Veterans Affairs
Health Systems Design & Development

Revision History

Date	Revision	Description	Contacts
November 2006	1.0	Release	**Project Manager and Analyst:** Dawn Clark
			Developer: Michael Ogi
			Technical Writer: Jim Alexander

Revision History

Table of Contents

List of Figures

List of Tables

1 Introduction

1.1 ESig Overview

As Health*e*Vet-VistA developers migrate VistA applications to modern technologies, interim solutions may be required until enterprise solutions are mature and stable. The Electronic Signature (ESig) service provides an interim solution for the use of electronic codes in place of wet signatures while Health*e*Vet-VistA's security infrastructure and architecture are being defined. The service duplicates for Java applications (J2EE or J2SE) the Kernel 8.0 electronic signature functionality currently used by VistA/M applications.

ESig furnishes a standard, consistent set of APIs that Health*e*Vet-VistA developers can implement to provide users access to electronic signature data stored on VistA/M systems. ESig APIs make calls from Java applications to VistA/M systems to retrieve, validate, and store electronic signature codes and signature block information (name, title, office phone, etc.). Additional Java APIs provide encoding/decoding, hash, and checksum calculation utilities, but do not interact with the VistA/M system.

Applications that implement the ESig service must provide a user interface (UI) to prompt users for their secret codes when authorizing orders, prescriptions, financial transactions, or other business processes. Users may also need the UI to create or modify their code or signature block data.

1.1.1 VistALink 1.5 Dependency

ESig requires the VistALink 1.5 service, which provides the transport layer enabling communication between a Java application and a VistA/M system.

The figure below shows ESig APIs communicating with VistA through VistALink 1.5. When a Health*e*Vet user signs on successfully, the connection from the application to VistA via VistALink is established. Consuming applications pass the VistaLinkConnection object to the ESig APIs that communicate with the VistA server.
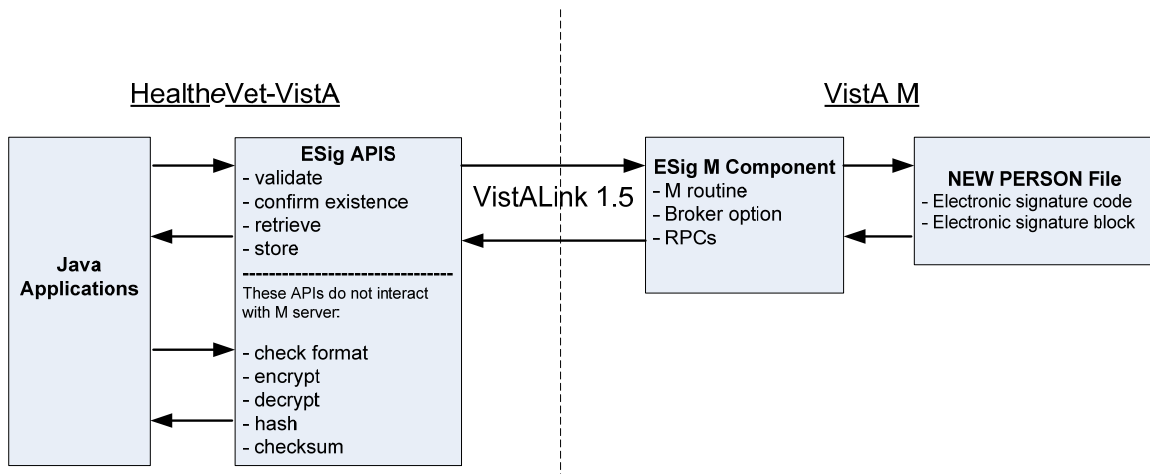
Figure 1-1. ESig Architecture

1.1.2 Installation

Health*e*Vet ESig consists of three parts:

- An M package containing a routine, a Broker option, and a set of Remote Procedures for accessing electronic signature codes and related data in the Kernel's NEW PERSON file

- A JAR file containing a set of Java APIs for passing and receiving electronic signature related information from M and for performing hashing, encryption, and decryption of strings. For ESig functionality to work, the ESig JAR file must be present on an application's classpath.

- Sample Java Swing, client console, and JSP utility applications to test or verify installation and configuration of the ESig components. These are included in the ESig distribution.

Although ESig is a Health*e*Vet-VistA application with Java and M components, **the only installation required by each IRM is the KIDS build on the VistA/M server**. Health*e*Vet-VistA applications requiring electronic signature functionality will include the ESig JAR file in their classpath. The JAR file contains APIs to perform ESig functions, including calling the VistA/M database.

Application developers and testers may want to deploy the sample ESig applications to client workstations (J2SE) or application servers (J2EE) to test the installation of the M server pieces. Instructions for deploying the sample applications are included in the *ESig 1.0 Developer Guide*.

1.2 Using this Guide

1.2.1 Purpose/Audience

This document provides instructions for installing the Electronic Signature 1.0 software on VistA/M servers. It is intended mainly for VistA/M system administrators. It will also be useful to Health*e*Vet-VistA application developers and anyone testing ESig functionality in Health*e*Vet applications.

This guide focuses on the VistA/M environment and assumes that readers are familiar with the following:

- VistA/M computing environment
- VA FileMan data structures and terminology
- M programming language
- Microsoft Windows

The instructions for using ESig's sample (test) J2SE and J2EE applications are included in the *ESig 1.0 Developer Guide*.

1.2.2 Text Conventions

The table below summarizes specialized use of typographical styles in this document.

Table 1-2. Text Conventions

Convention	Explanation	Example
ALL CAPS	M file, routine, variable, field, menu, field, and security key names.	Developers should be assigned the XUPROGMODE security key. The option [XOBE ESIG USER] may be added to the menu.
Boldface	Java file and directory names, particularly the first time they are mentioned in a passage.	Locate the **javadoc** folder and open your browser to the **index.html** file.
	Java GUI buttons.	Press **Enter**.
	Used in M dialog examples to show user entries.	`Enter a Host File:` **XOBE_1_.KID**
`Courier font`	Java class, method, or variable names	`ESigConnectionException`
<Angle brackets>	M key entries.	<Enter>
	In Java-related text, indicates information that is unknown or must be supplied by the user.	Locate the **jaas.config** file in the **<ESIG_SAMPLE_APP>** folder.

"Quotation marks"	Verbatim user entries in Java-related instructions.	You should name the file "log4j.xml".

The following symbols appear throughout the documentation to alert the reader to special information or conditions.

Symbol	Description
	Used to inform the reader of general information and reference material.
	Used to caution the reader to take special notice of critical information

1.3   Additional Resources

1.3.1 ESig Reference Materials

The following documents are included in the ESig documentation set:

- *ESig 1.0 Installation Guide* – Prerequisites and instructions for installing the ESig KIDS build on a VistA/M server.

- *ESig 1.0 Developer Guide* – Detailed information about ESig APIs and exceptions, for developers intending to use ESig APIs in their applications. Includes instructions useful to developers, quality assurance, and testers, for deploying sample J2EE (application server) and J2SE (client server) applications. These sample applications test the ESig APIs used by the host application.

- *ESig 1.0 System Management Guide* – M-side system and security information.

Because ESig APIs communicate with VistA/M systems through VistALink and Kernel RPCs, the following documentation is highly recommended:

- VistALink 1.5 documentation: *Developer Guide*, *Installation Guide*, and *System Management Guide*.

- RPC documentation: *RPC Broker Getting Started with the Broker Development Kit (BDK,) RPC Broker Developer's Guide* (i.e., BROKER.HLP, online help designed for programmers, distributed in the BDK)

- *Kernel v.8.0 Systems Manual*

ESig, VistALink, and RPC Broker documents are available on any of the Office of Information FTP directories as well as the VHA Document Library (VDL) at http://www.va.gov/vdl/.

1.3.2 Online Technical Information

1.3.2.1 <u>VistA/M Help</u>

After the ESig KIDS build is installed on the VistA/M server, developers and system administrators can use the standard Kernel/FileMan utilities for printouts of the installed components.

VistA software has online help and commonly used system default prompts. In roll-and-scroll mode users are strongly encouraged to enter question marks at any response prompt. At the end of the help display, you are immediately returned to the point from which you started. This is an easy way to learn about any aspect of VistA software.

To retrieve online documentation in the form of Help in VistA roll-and-scroll software:

- Enter a single question mark ("**?**") at a field/prompt to obtain a brief description. If a field is a pointer, entering one question mark ("**?**") displays the HELP PROMPT field contents and a list of choices, if the list is short. If the list is long, the user will be asked if the entire list should be displayed.

   A YES response will invoke the display. The display can be given a starting point by prefacing the starting point with an up-arrow ("**^**") as a response. For example, **^M** would start an alphabetic listing at the letter M instead of the letter A while **^127** would start any listing at the 127th entry.

- Enter two question marks ("**??**") at a field/prompt for a more detailed description. Also, if a field is a pointer, entering two question marks displays the HELP PROMPT field contents and the list of choices.

- Enter three question marks ("**???**") at a field/prompt to invoke any additional Help text that may be stored in Help Frames.

1.3.2.2 <u>VistA/M Data Dictionary Listings</u>

Technical information about files and the fields in files is stored in data dictionaries. To print formatted data dictionaries, reference the VA FileMan v.22.0 Advanced User Manual at http://www.va.gov/vdl.

1.3.2.3 <u>Javadocs</u>

Java class and package documentation is included in the ESig distribution file. Locate the **javadoc** folder and open your browser to the **index.html** file.

> ⓘ   To learn more about Javadoc files, refer to Sun's Javadoc Tool Home Page at: http://java.sun.com/j2se/javadoc/.

⚠️ **DISCLAIMER:** The appearance of external hyperlink references in this manual does not constitute endorsement by the Department of Veterans Affairs of the information, products, or services on the Website. The VHA does not exercise any editorial control over the information you may find at these locations.

2 Preliminary Considerations

ESig is installed as a KIDS build on the VistA/M server. Sites may wish to obtain only the KIDS file and the ESIG documentation. Office of Information developers and support teams should note a separate distribution zip file. The ESig distribution zip file includes optional sample applications to test the KIDS installation and configuration. These sample applications may also be useful examples for developers implementing the ESig service in their applications.

> ⚠ It is strongly recommended that you install the ESig KIDS build in a VistA/M server's Test account prior to installing it in a Production account.

2.1 ESig 1.0 Distribution Files

Table 2-1. Electronic Signature Distribution Files

File Name	Type	Description
XOBE_1_0IG.PDF	Binary	Installation Guide. Use in conjunction with the readme text file.
XOBE_1_0DG.PDF	Binary	Developer Guide.
XOBE_1_0SM.PDF	Binary	System Management Guide.
XOBE_1_0.KID	ASCII	KIDS Host File. Contains the Electronic Signature Vista/M server software: Server Routines Kernel Option and Remote Procedure Calls
XOBE_1_0.ZIP	Binary	Contains the client-side Java libraries, sample applications (J2SE and J2EE), the M server KIDS host file, and Javadoc reference information. The contents are: jars, javadoc, m, samples, readme

The ESig distribution zip file contains:

```
(root)
  ├── readme.txt (Provides any last minute changes, new instructions, and additional
  │              information to supplement the guides. Read all sections of this file
  │              prior to installation.)
  ├── jars/ (ESig JAR files)
  ├── javadoc/ (Javadocs for ESig APIs)
  ├── m/
  │   └── XOBE_1_0.KID (KIDS build for VistA/M server)
  └── samples/
      ├── J2EE/ (sample J2EE application)
      └── J2SE/ (sample client/server sample applications)
```

2.2 VistA/M Server Requirements

This section lists the minimum VistA/M server software required to install and use ESig.

2.2.1 Server Operating System and M Environment

ESig requires either of the following operating systems:

- Caché /NT

- Caché /VMS

2.2.2 Fully Patched Accounts

You should have both a Test account and a Production account for the ESig software. The account(s) must contain the *fully* patched versions of the software listed in following table.

Table 2-2. Required Fully Patched M Accounts

Software	Version	Patch Information
Kernel	8.0	Fully patched.
Kernel Toolkit	7.3	Fully patched
RPC Broker	1.1	Fully patched.
VA FileMan	22.0	Fully patched.
VistALink	1.5	Fully patched.

These packages must be properly installed and fully patched prior to installing the Electronic Signature VistA/M server software distribution. Patches must be installed in published sequence.

VistALink 1.5 is a collection of three separate packages under the XOB* namespace: Foundations 1.5 (XOBU); VistALink 1.5 (XOBV); and VistALink Security 1.5 (XOBS).

2.2.3 Network Communications Software

One or more properly configured VistALink 1.5 listeners must be running as a TCP/IP VMS service on your VistA/M server(s)

2.3 User Requirements

IRM support staff responsible for installing ESig on VistA/M servers (and optionally, client workstations) should be familiar with the following areas:

- VistA computing environment

- Installing software and managing a VistA/M system

- Setting up a VistALink 1.5 listener and ensuring the service is enabled

- Kernel Installation and Distribution System (KIDS)

- VA FileMan data structures and terminology

- Microsoft Windows

- Red Hat Linux

- M programming language

3 Installing ESig on the VistA/M Server

Be sure to check the **readme.txt** file included in the Electronic Signature distribution zip file for the most recent installation instructions.

Electronic Signature requires a VistALink 1.5 listener.

The instructions in this section are applicable for the Test/Production accounts in Caché/NT and Caché/VMS environments.

Check the FORUM Patch Module and make any new patches that have been released by the applications listed in section 2.2.2 readily available, so that you can apply them before you begin the Electronic Signature installation process.

There are three VistALink 1.5 packages loaded in the FORUM Patch Module: Foundations, VistALink, and VistALink Security.

3.1   FTPing the XOBE_1_0.KIDS File to the M Server

IRM staff tasked with installation and support of the Esig package are only responsible for the VistA/M installation activities described here. You'll need the XOBE_1_0.KID file, the VistA/M server software in Kernel 8.0 KIDS format. It is available from the OI ANONYMOUS.SOFTWARE directories. FTP the KIDS file to your VistA/M system in ASCII format only. The file is also exported in the **m** folder of the Electronic Signature distribution zip file.

3.2   Installing the ESig KIDS Build

Use KIDS to install the Electronic Signature routine, option, and remote procedures. From the KIDS menu you will use the following sequence of options:

1. Load a Distribution: Use the host file name, XOBE_1_0.KID

2. Verify Checksums in Transport Global: Use the install name, XOBE 1.0

3. Backup a Transport Global: Use the install name, XOBE 1.0

4. Install Package(s): Use the install name, XOBE 1.0

During the installation of the package in step 4 above, you will be asked three questions. Answer **NO** to all of them:

```
Want KIDS to Rebuild Menu Trees Upon Completion of Install? YES// NO
Want KIDS to INHIBIT LOGONs during the install? YES // NO
Want to DISABLE Scheduled Options, Menu Options,
   and Protocols? YES// NO
```

Installation will take less than one minute. No options need to be placed out of order, and users can remain on the system. Production system installations will generate a MailMan message to update the FORUM National Patch/Package Tracking module for your site.

ℹ See Appendix A of this guide for an example of the KIDS installation.

3.3   Verifying the Checksum Value

Use the Kernel Toolkit 8.0 checksum utility to verify the checksums of the XOBE* routine(s) installed. From the programmer prompt:

```
>D CHECK1^XTSUMBLD

New CheckSum CHECK1^XTSUMBLD:

This option determines the current checksum of selected routine(s).
The Checksum of the routine is determined as follows:

1. Any comment line with a single semi-colon is presumed to be
   followed by comments and only the line tag will be included.

2. Line 2 will be excluded from the count.

3. The total value of the routine is determined (excluding
   exceptions noted above) by multiplying the ASCII value of each
   character by its position on the line and position of the line in
   the routine being checked.

     Select one of the following:

          P         Package
          B         Build

Build from: Build

This will check the routines from a BUILD file.
Select BUILD NAME: XOBE 1.0        ELECTRONIC SIGNATURE
XOBESIG   value = 35924230
done
```

ℹ The checksum value obtained should be "35924230," as shown above.

3.4 Assigning the User Context Menu

The **Context for Electronic Signature Users [XOBE ESIG USER]** option is a Broker (Client/Server) option that contains the remote procedures used by ESig. To use the remote procedures, at least one of the following must be true:

- The user must have the [XOBE ESIG USER] Broker option added to his or her secondary menu.

- The [XOBE ESIG USER] Broker option must be added to the Common Menu [XUCOMMAND] in Kernel. In this case, all users on the system would have access to the ESig options; the Broker option need not be assigned specifically to individual users.

- The user must be defined as a programmer on the VistA/M system.

The recommended procedure for giving users access to the ESig remote procedures is to add the [XOBE ESIG USER] Broker option to the Common Menu [XUCOMMAND] in Kernel.

This concludes the Esig installation activities.

Appendix A: Sample KIDS Installation

The following is an example of an M-side Electronic Signature software installation in a VistA/M test or mirror account.

```
Select Kernel Installation & Distribution System Option: INstallation

    1       Load a Distribution
    2       Verify Checksums in Transport Global
    3       Print Transport Global
    4       Compare Transport Global to Current System
    5       Backup a Transport Global
    6       Install Package(s)
            Restart Install of Package(s)
            Unload a Distribution

Select Installation Option: 1  Load a Distribution
Enter a Host File: XOBE_1_0.KID

KIDS Distribution saved on Sep 27, 2005@08:03:32
Comment: Electronic Signature v1.0 [Build 1.0.0.024]

This Distribution contains Transport Globals for the following Package(s):
   XOBE 1.0
Distribution OK!

Want to Continue with Load? YES// <Enter>
Loading Distribution...

   XOBE 1.0
Use INSTALL NAME: XOBE 1.0 to install this Distribution.
```

```
    1       Load a Distribution
    2       Verify Checksums in Transport Global
    3       Print Transport Global
    4       Compare Transport Global to Current System
    5       Backup a Transport Global
    6       Install Package(s)
            Restart Install of Package(s)
            Unload a Distribution

Select Installation Option: 2  Verify Checksums in Transport Global
Select INSTALL NAME: XOBE 1.0      Loaded from Distribution  11/22/05@15:13:20
    => Electronic Signature v1.0 [Build 1.0.0.024]  ;Created on Sep 27, 2005@

This Distribution was loaded on Nov 22, 2005@15:13:20 with header of
   Electronic Signature v1.0 [Build 1.0.0.024]  ;Created on Sep 27,
2005@08:03:32
   It consisted of the following Install(s):
      XOBE 1.0
DEVICE: HOME// <Enter>

PACKAGE: XOBE 1.0     Nov 22, 2005 3:13 pm                          PAGE 1
-------------------------------------------------------------------------------

   1 Routine checked, 0 failed.
```

Appendix A: Sample KIDS Installation

```
    1        Load a Distribution
    2        Verify Checksums in Transport Global
    3        Print Transport Global
    4        Compare Transport Global to Current System
    5        Backup a Transport Global
    6        Install Package(s)
             Restart Install of Package(s)
             Unload a Distribution

Select Installation Option: 5  Backup a Transport Global
Select INSTALL NAME: XOBE 1.0        Loaded from Distribution  11/22/05@15:13:20
     => Electronic Signature v1.0 [Build 1.0.0.024]  ;Created on Sep 27, 2005@

This Distribution was loaded on Nov 22, 2005@15:13:20 with header of
   Electronic Signature v1.0 [Build 1.0.0.024]  ;Created on Sep 27, 2005@08:03:3
2
   It consisted of the following Install(s):
       XOBE 1.0
Subject: Backup of XOBE 1.0 install on Nov 22, 2005
  Replace <Enter>
Loading Routines for XOBE 1.0.
Send mail to: INSTALLER,TEST
Select basket to send to: IN// <Enter>
And Send to: <Enter>
```

```
    1        Load a Distribution
    2        Verify Checksums in Transport Global
    3        Print Transport Global
    4        Compare Transport Global to Current System
    5        Backup a Transport Global
    6        Install Package(s)
             Restart Install of Package(s)
             Unload a Distribution

Select Installation Option: 6  Install Package(s)
Select INSTALL NAME: XOBE 1.0        Loaded from Distribution  11/22/05@15:13:20
     => Electronic Signature v1.0 [Build 1.0.0.024]  ;Created on Sep 27, 2005@

This Distribution was loaded on Nov 22, 2005@15:13:20 with header of
   Electronic Signature v1.0 [Build 1.0.0.024]  ;Created on Sep 27, 2005@08:03:3
2
   It consisted of the following Install(s):
       XOBE 1.0
Checking Install for Package XOBE 1.0

Install Questions for XOBE 1.0


Want KIDS to Rebuild Menu Trees Upon Completion of Install? YES// NO


Want KIDS to INHIBIT LOGONs during the install? YES// NO
Want to DISABLE Scheduled Options, Menu Options, and Protocols? YES// NO

Enter the Device you want to print the Install messages.
You can queue the install by enter a 'Q' at the device prompt.
Enter a '^' to abort the install.

DEVICE: HOME// <Enter>

                               XOBE 1.0
────────────────────────────────────────────────────────────────────────────────
```

```
 Install Started for XOBE 1.0 :
               Nov 22, 2005@15:13:44

Build Distribution Date: Sep 27, 2005

 Installing Routines:
               Nov 22, 2005@15:13:44

 Installing PACKAGE COMPONENTS:

 Installing REMOTE PROCEDURE

 Installing OPTION
               Nov 22, 2005@15:13:44

 Updating Routine file...

 Updating KIDS files...

 XOBE 1.0 Installed.
               Nov 22, 2005@15:13:44

 Not a production UCI

 NO Install Message sent


_____

   100%                    25              50              75
Complete

 XOBE 1.0 Installed.
               Nov 22, 2005@15:13:44

 Not a production UCI

 NO Install Message sent

Install Completed
```

Appendix A: Sample KIDS Installation

Glossary

Term	Definition
Access Code	A code, that along with the Verify code allows the Kernel to identify a user as authorized to gain access to a VistA system.
API	Application Programming Interface. The set of public classes a package uses. Intended to prevent duplication of utilities and limit the number of callable entry points.
ASCII	American Standard Code for Information Interchange
Authentication	Verification of a user's identity.
Authorization	Checking the permissions of a user to allow or disallow the performance of some function.
CCE	Computer Code Entry. A password/PIN technology for asserting electronic signature intent in a health-care environment. Computer Code Entry (CCE) is explicitly endorsed in existing medical records practice/regulation and is permitted by JCAHO IM7 standards.
Client	A single term used interchangeably to refer to a user, the workstation (e.g., PC), and the portion of the software that runs on the workstation.
Data Dictionary	The structure of a file, table, or group of related information as defined for and by VA FileMan
Database Integration Agreement (DBIA)	A formal, documented understanding between two or more application packages that describes how data is shared or information is exchanged. The Database Administrator (DBA) maintains these agreements. Documented agreements are available via the DBIA menu on FORUM
DBA	Data Base Administrator
Decrypt	To decipher, decode, or unlock encrypted or encoded messages/data to make them readable.
DUZ	DUZ represents the internal entry number (IEN) for a user's record in File #200, the New Person file and is designated as a system-wide variable in the VistA environment. DUZ is used as a re-authentication mechanism.
EAR	Enterprise ARchive file.
EJB	Enterprise Java Bean.
Electronic Signature	A secret, user-supplied PIN or code that is used to authorize business processes and is a legally binding equivalent of an individual's handwritten signature. For the VA Kernel 8.0 an electronic signature must be 6-20 characters in length and can contain letters, numbers, and punctuation.
Encrypt	To encode messages or data so that they are unreadable unless they are decoded.
ESig	Electronic Signature.
EVS	Enterprise VistA Support
FOIA	Freedom of Information Act
FTP	File Transfer Protocol
GUI	Graphical User Interface. The graphical elements on the screen through which the user interacts with the computer.
Hash	To encrypt data by substituting a shorter fixed-length value or key to represent the original. Hashing algorithms are one-way functions, so that it is not possible to decrypt the substitute values to generate the original data.
IP	Internet Protocol

Glossary

Term	Definition
IRM	Information Resources Management. A service at each VAMC responsible for computer management and system security.
ISO	Information Security Officer
J2EE	Java ^{TM} 2 Platform, Enterprise Edition
J2SE	Java 2 Standard Edition
JAAS	Java Authentication and Authorization Service
Javadoc	Javadoc is the tool from Sun Microsystems for generating API documentation in HTML format from doc comments in Java source code.
JNDI	Java Naming Directory Interface
JSP	Java Server Page
JVM	Java Virtual Machine
Kernel	VA Kernel 8.0 is a suite of VistA software that provides a standard and consistent user and programmer interface between application packages, the OS, and users.
M	MUMPS
Option	A selectable software function: a menu item.
PIN	Personal Identification Number
PKI	Public Key Infrastructure
RPC	Remote Procedure Call
SAC	Standards and Conventions
SACC	Standards and Conventions Committee
SDK	Java Software Development Kit. APIs and tools for developing applications.
Signature Block	Data associated with an electronic signature user, stored in the New Person file. Signature block data consists of the user's initials, printed name, title, office phone, voice pager, and digital pager.
TBD	To Be Determined
TCP/IP	Transmission Control Protocol / Internet Protocol
URL	Uniform Resource Locator
User	This term generally refers to VA employees and volunteers with active records established in File #200, the New Person file, who are authorized to access a VistA system.
VA	Veterans Affairs
VA ITSCAP	VA Information Technology Security Certification and Accreditation Program (VA Directive 6214)
VAMC	Department of Veterans Affairs Medical Center
VAX	VAX (Virtual Address eXtension) is an established line of mid-range server computers from the Digital Equipment Corporation (DEC).
VHA	Veterans Health Administration
VistA	Veterans Health Information Systems and Technology Architecture
VistA/M Server	The computer where the M data and the RPC Broker remote procedure calls (RPCs) reside.
VistALink	A standardized, portable, and secure mechanism for establishing connections between Java (J2SE and J2EE) and VistA/M servers.

Term	Definition
VMS	Virtual Machine System (operating system for VAX computers)
WAN	Wide Area Network
WAR	Web ARchive
WLS	WebLogic Server
XML	Extensible Markup Language