Electronic Signature (ESig)

**Version 1.0**

System Management 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:** REDACTED**Developer:** REDACTED**Technical Writer:** REDACTED  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Table of Contents

[1 Introduction 1](#_Toc150655796)

[1.1 ESig Overview 1](#_Toc150655797)

[1.1.1 VistALink 1.5 Dependency 1](#_Toc150655798)

[1.1.2 Installation 2](#_Toc150655799)

[1.2 Using this Guide 3](#_Toc150655800)

[1.2.1 Purpose 3](#_Toc150655801)

[1.2.2 Audience 3](#_Toc150655802)

[1.2.3 Text Conventions 3](#_Toc150655803)

[1.3 Additional Resources 4](#_Toc150655804)

[1.3.1 ESig Reference Materials 4](#_Toc150655805)

[1.3.2 Online Technical Information 5](#_Toc150655806)

[2 VistA/M Information 7](#_Toc150655807)

[2.1 ESig 1.0 Installation 7](#_Toc150655808)

[2.2 Site Parameters 7](#_Toc150655809)

[2.3 Performance and Scalability 7](#_Toc150655810)

[2.4 Exported Files 7](#_Toc150655811)

[2.5 Global Translation, Journaling, and Protection 7](#_Toc150655812)

[2.6 VistA/M Server Routines 7](#_Toc150655813)

[2.6.1 Routine Definitions 7](#_Toc150655814)

[2.6.2 Routine Mapping 7](#_Toc150655815)

[2.6.3 Menu Option 8](#_Toc150655816)

[2.7 Exported Remote Procedures 8](#_Toc150655817)

[2.8 Callable Routines, Entry Points, and APIs 9](#_Toc150655818)

[2.9 External Relations 9](#_Toc150655819)

[2.9.1 Software Requirements 9](#_Toc150655820)

[2.9.2 DBA Approvals and Integration Agreements (IAs) 9](#_Toc150655821)

[2.10 Internal Relations 11](#_Toc150655822)

[2.10.1 Internal Relations 11](#_Toc150655823)

[2.10.2 Namespace 11](#_Toc150655824)

[2.11 Package-Wide Variables 11](#_Toc150655825)

[3 ESig Security Features 13](#_Toc150655826)

[3.1 VHA Directives, Policies, and Legal Requirements 13](#_Toc150655827)

[3.2 Mail Groups and Alerts 13](#_Toc150655828)

[3.3 Archiving and Purging 13](#_Toc150655829)

[3.4 Contingency Planning 13](#_Toc150655830)

[3.5 Interfacing 13](#_Toc150655831)

[3.6 Menus 14](#_Toc150655832)

[3.7 Security Keys 14](#_Toc150655833)

[3.8 Files 14](#_Toc150655834)

[3.9 RPC Security 14](#_Toc150655835)

[Glossary 15](#_Toc150655836)

List of Figures

[Figure 1-1. ESig Architecture 2](#_Toc149120241)

List of Tables

[Table 1-2. Text Conventions 3](#_Toc150655855)

[Table 2-1. ESig 1.0 Distributed Remote Procedures 8](#_Toc150655856)

[Table 2-2. Required VistA Software 9](#_Toc150655857)

# Introduction

## 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.

### 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

### 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, the only installation requiredis 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*.

## Using this Guide

### Purpose

This document provides technical reference data for the Health*e*Vet -VistA ESig 1.0 package, primarily on the M side. The *ESig 1.0 Installation Guide* presents instructions for the two administrative tasks required by ESig 1.0:

* Installing the ESig KIDS build on a VistA/M server
* Deploying the ESig sample applications on a BEA WebLogic application server and client workstation.

Managing electronic signature code data is a Kernel function; for pertinent information see Chapter 4 (“Electronic Signature Codes”) of the *Kernel v8.0 Systems Manual*.

### Audience

This document is for the use of Health*e*Vet-VistA application developers, testing and quality-assurance personnel, Enterprise VistA Support (EVS) personnel, IRM staff, and data center M administrators. It focuses on the 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

### 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 |

## Additional Resources

### 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/>.

### Online Technical Information

#### VistA/M Help

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.

#### VistA/M Data Dictionary Listings

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

#### Javadocs

Java class and package documentation is included in the ESig distribution zip 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.  |

# VistA/M Information

## ESig 1.0 Installation

The *ESig 1.0 Installation Guide* provides detailed installation information. It also contains requirements and recommendations to configure ESig 1.0. This document (XOBE\_1\_OIG.PDF) is available on the Office of Information ANONYMOUS.SOFTWARE directories and the VHA Document Library (<http://www.va.gov/vdl>).

## Site Parameters

There are no ESig 1.0 site parameters.

## Performance and Scalability

Current performance statistics are limited. However, preliminary testing results indicate that the processing time and resources consumed by ESig itself are minimal. ESig uses VistALink to communicate with the VistA/M server, and VistALink does not introduce any additional overhead to messages sent between the client and the VistA/M server.

## Exported Files

No new files are exported to the VistA/M server for ESig 1.0 software. Applications using the ESig APIs will be responsible for deploying the libraries required for ESig to their BEA WebLogic application server(s).

## Global Translation, Journaling, and Protection

ESig 1.0 software introduces no new globals on the VistA/M server. Translation, journaling, and protection are not applicable.

## VistA/M Server Routines

### Routine Definitions

ESig distributes just one M routine:

**XOBESIG –** This routine contains the code for the Remote Procedure Calls (RPCs) to retrieve and save electronic signature codes and related data on the VistA/M server.

### Routine Mapping

Routine mapping is at the discretion of the systems manager. ESig has no requirements for routine mapping.

### Menu Option

**Name** [**XOBE ESIG USER]**

**Menu Text** Context for Electronic Signature Users

**Type** Broker (Client / Server)

**Description** This option is the user context that contains the RPCs used by ESig. Users of a HealtheVet application that calls ESig RPCs must have this option assigned to their VistA menu tree.

|  |  |
| --- | --- |
|  | To bypass security for development purposes, developers should be assigned the XUPROGMODE security key*.* Holders of XUPROGMODE can run any VistA client / server application (regardless of menu trees) and access any RPC without regard to application context. |

|  |  |
| --- | --- |
|  | To simplify maintenance, the option [XOBE ESIG USER] may be added to the Common [XUCOMMAND] menu on the VistA/M server to automatically give all users on that server access to the electronic signature remote procedures. |

## Exported Remote Procedures

ESig 1.0 distributes the remote procedures detailed in the table below.

Table 2-1. ESig 1.0 Distributed Remote Procedures

|  |  |  |  |
| --- | --- | --- | --- |
| **Remote Procedure** | **Description** | **Routine** | **Return Value Type** |
| XOBE ESIG GET CODE | Returns the electronic signature code for the user from the NEW PERSON file. | GETCODE^XOBESIG | Single Value |
| **XOBE ESIG GET DATA** | Returns the data for the electronic signature block-related fields from the NEW PERSON file. | GETDATA^XOBESIG | Array |
| XOBE ESIG IS DEFINED | Returns whether the user currently has an electronic signature code defined. This RPC returns “0” if the electronic signature code is null; it returns “1” if the user’s electronic signature code is defined. | ISDEF^XOBESIG | Single Value |
| XOBE ESIG SET CODE | Saves the user's electronic signature code in the NEW PERSON file. | SETCODE^XOBESIG | Single Value |
| XOBE ESIG SET DATA | Saves the electronic signature block-related data in the NEW PERSON file. | SETDATA^XOBESIG | Array |

## Callable Routines, Entry Points, and APIs

ESig 1.0 does not provide any callable M routines. However, it does provide Java programming interfaces.

|  |  |
| --- | --- |
|  | For information on the ESig Java programming interfaces, see the “ESig APIs”chapter of the *Electronic Signature Developer Guide*. |

## External Relations

### Software Requirements

ESig 1.0 relies on the VistA software listed in the table below.

Table 2-2. Required VistA Software

|  |  |  |
| --- | --- | --- |
| **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 |

### DBA Approvals and Integration Agreements (IAs)

The VistA Database Administrator (DBA) maintains a list of Integration Agreements (IAs). IAs are mutual agreements between software developers that allow the use of internal entry points or other software-specific features that are not available to the general programming public.

#### Obtaining Integration Agreement Information

**To obtain a current list of any IAs to which the ESig 1.0 software (XOBE) is a custodian:**

1. Sign on to the FORUM system REDACTED
2. Go to the DBA menu [DBA].
3. Select the Integration Agreements Menu option [DBA IA ISC].
4. Select the Custodial Package Menu option [DBA IA CUSTODIAL MENU].
5. Choose the ACTIVE by Custodial Package option [DBA IA CUSTODIAL].
6. When this option prompts you for a package, enter **ELECTRONIC SIGNATURE or XOBE.**
7. All current IAs to which the ESig software is a custodian will be listed.

**To obtain detailed information on a specific integration agreement:**

1. Sign on to the FORUM system REDACTED
2. Go to the DBA menu [DBA].
3. Select the Integration Agreements Menu option [DBA IA ISC]
4. Select the Inquire option [DBA IA INQUIRY].
5. When prompted for "INTEGRATION REFERENCES," enter the specific integration agreement number of the IA you would like to display.
6. The option will display the full text of the IA you requested.

**To obtain the current list of IAs, if any, to which the ESig software is a subscriber:**

1. Sign on to the FORUM system REDACTED
2. Go to the DBA menu [DBA].
3. Select the Integration Agreements Menu option [DBA IA ISC].
4. Select the Subscriber Package Menu option [DBA IA SUBSCRIBER MENU]
5. Choose the Print ACTIVE by Subscribing Package option [DBA IA SUBSCRIBER]
6. When prompted with "START WITH SUBSCRIBING PACKAGE," enter ELECTRONIC SIGNATURE (in uppercase). When prompted with "GO TO SUBSCRIBING PACKAGE," enter ELECTRONIC SIGNATURE (in uppercase).
7. All current IAs to which the ESig software is a subscriber will be listed

#### ESig-Kernel Integration Agreement

The following is the integration agreement ESig has with Kernel to access fields in the New Person file:

 4297 NAME: ELECTRONIC SIGNATURE-RELATED DATA IN THE NEW PERSON FILE

 CUSTODIAL PACKAGE: KERNEL REDACTED

SUBSCRIBING PACKAGE: ELECTRONIC SIGNATURE REDACTED

 USAGE: Private ENTERED: DEC 23,2003

 STATUS: Active EXPIRES:

 DURATION: Till Otherwise Agr VERSION:

 FILE: 200 ROOT: VA(200,

 DESCRIPTION: TYPE: File

 Electronic Signature is a collection of Java APIs to validate, retrieve,

 and save electronic signature codes and related data on the M server, as

 well as APIs to encrypt and decrypt strings similar to the APIs provided

 by the existing VA Kernel 8.0 electronic signature APIs.

 The Java APIs provide HSD&D developers that are rehosting their

 applications to a new Java environment a standardized method for migrating

 their electronic signature functionality. It is hoped that this will

 reduce duplication of effort, promote more efficient use of limited

 development resources, and satisfy the VistA user's business needs.

 This IA permits Electronic Signature to access electronic

 signature-related data in the NEW PERSON file (#200) as listed in the

 GLOBAL REFERENCE section of this Integration Agreement. All fields are

 accessed via VA FileMan calls, such as $$GET1^DIQ and FILE^DIE, rather

 than direct global reads.

 ^VA(200,

 .132 OFFICE PHONE .13;2 Both R/W w/Fileman

 .137 VOICE PAGER .13;7 Both R/W w/Fileman

 .138 DIGITAL PAGER .13;8 Both R/W w/Fileman

 1 INITIAL 0;2 Both R/W w/Fileman

 20.2 SIGNATURE BLOCK PRIN 20;2 Both R/W w/Fileman

 20.3 SIGNATURE BLOCK TITL 20;3 Both R/W w/Fileman

 20.4 ELECTRONIC SIGNATURE 20;4 Both R/W w/Fileman

 ROUTINE:

## Internal Relations

### Internal Relations

No routines, files or options within the ESig product assume that the entry / exit logic of another option has already occurred.

### Namespace

ESig has been assigned the **XOBE** namespace. The XOBE namespace is a member of the Foundations (XOB\*) product family.

## Package-Wide Variables

ESig does not create any package-wide variables that have received Standards and Convention Committee (SACC) exemptions.

# ESig Security Features

Electronic Signature security features are based on the following requirements:

* **HeV applications authenticate their users.**

HeV applications are required to authorize and authenticate their users. Infrastructure tools such as KAAJEE (Kernel Authentication and Authorization for J2EE) and FatKAAT (rich-client Kernel Authentication and Authorization) are mandated for use in Health*e*Vet -VistA Web-based and rich-client applications, respectively.

* **Users must have valid Access and Verify codes.**
* **Health*e*Vet -VistA applications must have a valid VistALink connection request.**
* **Any remote procedure call must be registered and valid for the application being executed.**
* **Users must have assigned to their VistA menu tree the Context for Electronic Signature Users [XOBE ESIG USER] “B”-type option.**

## VHA Directives, Policies, and Legal Requirements

The pending *VHA Directive on Modifications to VistA and VistA Sensitive Software* prohibits modification of any part of the ESig software. There are no special legal requirements that pertain to the use of ESig. Distribution of ESig software is unrestricted.

## Mail Groups and Alerts

ESig does not make use of mail groups or alerts.

## Archiving and Purging

ESig does not have any archiving or purging requirements or features.

## Contingency Planning

It is the responsibility of the using service to develop a local contingency plan for use in the event of application problems.

## Interfacing

Please see the sections “[External Relations](#_External_Relations)”(VistA/M-server side) and “Required Java Software” (Java client side) in the Electronic Signature Developer Guide for a list of external packages required by ESig.

## Menus

There are no options of special note for Information Security Officers (ISOs) to view.

## Security Keys

ESig requires nospecific security keys. However, to bypass security for development purposes, we recommend client/server application developers be assigned the XUPROGMODE security key. All users assigned the XUPROGMODE security key can do the following:

* Run any VistA client/server application regardless of whether or not it is in their menu tree
* Access any RPC without regard to the application context

## Files

ESig exports no files.

## RPC Security

For information regarding security enforced on RPCs, please visit the Infrastructure section of the VHA Document Library to access the *RPC Broker Systems Manual*:

<http://www.va.gov/vdl/>

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