

---

# VMS Authentication Module Administration and User's Guide

**March 2006**

This manual provides the system manager with the procedures for installing, managing, and using the VAM family of software products.

**Revision/Update:** This is a new manual.

**Operating System/Version:** OpenVMS VAX V7.3 and higher  
OpenVMS Alpha V6.2 and higher  
OpenVMS I64 8.2 and higher

**MultiNet Version:** V4.4 and later  
**TCPware Version:** V5.6-2 and later  
**UCX Version:** V4.0 ECO 5 and later  
**TCP/IP Services Version:** V5.0 and later

**RSA Authentication  
Manager Version:** V6.0 and later

**Software Version:** V1.0

**Process Software  
Framingham, Massachusetts  
USA**

---

The material in this document is for informational purposes only and is subject to change without notice. It should not be construed as a commitment by Process Software. Process Software assumes no responsibility for any errors that may appear in this document.

Use, duplication, or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

The following third-party software may be included with your product and will be subject to the software license agreement.

Portions Copyright © 1993 by Hewlett-Packard Corporation.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies, and that the name of Hewlett-Packard Corporation not be used in advertising or publicity pertaining to distribution of the document or software without specific, written prior permission. THE SOFTWARE IS PROVIDED "AS IS" AND HEWLETT-PACKARD CORPORATION DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL HEWLETT-PACKARD CORPORATION BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

ACE/Agent, ACE/Server, Because Knowledge is Security, BSAFE, ClearTrust, Confidence Inspired, e-Titlement, Intelli-Access, Keon, RC2, RC4, RC5, RSA, the RSA logo, RSA Secured, the RSA Secured logo, RSA Security, SecurCare, SecurID, SecurWorld, Smart Rules, The Most Trusted Name in e-Security, Transaction Authority, and Virtual Business Units are either registered trademarks or trademarks of RSA Security Inc. in the United States and/or other countries.

All other goods and/or services mentioned are trademarks of their respective companies Secure Shell (SSH). Copyright © 2000. This License agreement, including the Exhibits ("Agreement"), effective as of the latter date of execution ("Effective Date"), is hereby made by and between Data Fellows, Inc., a California corporation, having principal offices at 675 N. First Street, 8th floor, San Jose, CA 95112170 ("Data Fellows") and Process Software, Inc., a Massachusetts corporation, having a place of business at 959 Concord Street, Framingham, MA 01701 ("OEM").

All other trademarks, service marks, registered trademarks, or registered service marks mentioned in this document are the property of their respective holders.

Copyright ©1997, 1998, 1999, 2000 Process Software Corporation. All rights reserved. Printed in USA.

Copyright ©2006 Process Software. All rights reserved. Printed in USA.

If the examples of URLs, domain names, internet addresses, and web sites we use in this documentation reflect any that actually exist, it is not intentional and should not to be considered an endorsement, approval, or recommendation of the actual site, or any products or services located at any such site by Process Software. Any resemblance or duplication is strictly coincidental.

---

# Contents

## Preface

|   |      |
|---|------|
| About VMS Authentication Module .....       | v    |
| Introducing This Guide.....                 | v    |
| What You Need to Know Beforehand .....      | v    |
| How This Guide Is Organized .....           | v    |
| Online Help.....                            | vi   |
| Accessing the VAM Public Mailing List ..... | vi   |
| Obtaining Customer Support .....            | vii  |
| License Information.....                    | vii  |
| Maintenance Services .....                  | vii  |
| Reader's Comments Page.....                 | viii |
| Documentation Set.....                      | viii |
| Conventions Used.....                       | ix   |

## Chapter 1 Before You Begin

|  |     |
|--|-----|
| Introduction.....                            | 1-1 |
| Steps to Get VAM Up and Running.....         | 1-1 |
| Prepare for Installation .....               | 1-2 |
| Hardware Requirements .....                  | 1-2 |
| Software Requirements.....                   | 1-2 |
| Disk Space and Global Pages .....            | 1-2 |
| General Requirements .....                   | 1-2 |
| Where to Install VAM.....                    | 1-2 |
| Release Notes and Online Documentation ..... | 1-3 |

## Chapter 2 Installing and Configuring VAM

|   |     |
|---|-----|
| Introduction.....   | 2-1 |
| Load the Software.....  | 2-1 |
| Start VMSINSTAL .....   | 2-2 |
| Sample Installation .....   | 2-2 |
| Installing VAM for the First Time on a Common VMScluster System Disk..... | 2-4 |
| Installing VAM on Mixed Platform Clusters .....                           | 2-4 |

|  |     |
|--|-----|
| Post-Installation Steps .....  | 2-4 |
| Post-Installation Using the SecurID or Local UAF VAM Callable Module ..... | 2-4 |
| Post-Installation Using the SecurID VAM OpenVMS LOGINOUT Callouts .....    | 2-4 |
| Optional Post-Installation Steps .....                                     | 2-5 |

## **Chapter 3 Using VAM**

|  |     |
|--|-----|
| Introduction .....                                   | 3-1 |
| The VAM API .....                                    | 3-1 |
| The API Authentication Philosophy .....              | 3-1 |
| Controlling LOCALUAF Access to the Application ..... | 3-2 |
| The VAM LGI Callouts .....                           | 3-3 |
| Sample VAM Login .....                               | 3-3 |
| Controlling Access to the Callout .....              | 3-4 |
| Other VAM-Specific Logical Names .....               | 3-4 |
| General Logicals .....                               | 3-4 |
| Logging Control Logicals .....                       | 3-5 |
| SecurID Files Used by VAM.....                       | 3-5 |

## **Chapter 4 Using the VAM API**

|                                   |     |
|-----------------------------------|-----|
| Introduction .....                | 4-1 |
| Compiling a VAM Application ..... | 4-1 |
| Linking A VAM Application.....    | 4-1 |
| VAM API Functions .....           | 4-1 |
| VMSAuthenticate .....             | 4-2 |
| IOCallback.....                   | 4-4 |
| InfoCallback .....                | 4-6 |
| TimeoutCallback .....             | 4-7 |
| ScreenClearCallback .....         | 4-8 |

---

# Preface

## About VMS Authentication Module

The VMS Authentication Module (VAM) provides users of OpenVMS systems controlled access to both user-written applications and the OpenVMS system overall using SecurID. It can be incorporated into an OpenVMS-based platform in two ways:

- Via an API that the user incorporates into a specific application to control access to that application
- On a system-wide basis via use of the LGI callouts for OpenVMS LOGINOUT.EXE.

Chapter 3, *Using VAM*, describes the two mechanisms and how they are implemented.

## Introducing This Guide

This guide describes the VMS Authentication Module (VAM) software. It covers the following topics: software installation, configuration, and server monitoring and control.

## What You Need to Know Beforehand

Before using VAM, you should be familiar with:

- Computer networks in general
- OpenVMS operating system and file system
- The TCP/IP stack (MultiNet, TCPware, or HP's OpenVMS TCP/IP software) you're using

## How This Guide Is Organized

This guide has the following contents:

- Chapter 1, *Before You Begin*, explains what you need to prepare for an installation.
- Chapter 2, *Installing VAM*, provides a step-by-step procedure for executing the software installation.
- Chapter 3, *Using VAM*, explains how to configure VAM authentication options.
- Chapter 4, *Using the VAM API*, describes how to integrate the VAM API into a user-written application.

## Online Help

There is no online help for VAM.

## Accessing the VAM Public Mailing List

Process Software maintains two public mailing lists for VAM customers:

- **Info-VAM@process.com**
- **VAM-Announce@process.com**

The **Info-VAM@process.com** mailing list is a forum for discussion among VAM system managers and programmers. Questions and problems regarding VAM can be posted for a response by any of the subscribers. To subscribe to info-VAM, send a mail message with the word “SUBSCRIBE” in the body to Info-VAM-request@process.com.

You can retrieve the Info-VAM archives by anonymous FTP to ftp.multinet.process.com. The archives are located in the directory [MAIL\_ARCHIVES.INFO-VAM].

The **VAM-Announce@process.com** mailing list is a one-way communication (from Process Software to you) used for the posting of announcements relating to VAM (patch releases, product releases, etc.). To subscribe to VAM-Announce, send a mail message with the word “SUBSCRIBE” in the body to VAM-Announce-request@process.com.

---

## Obtaining Customer Support

You can use the following customer support services for information and help about VAM and other Process Software products if you subscribe to our Product Support Services. (If you bought VAM products through an authorized Process Software reseller, contact your reseller for technical support.) Contact Technical Support directly using the following methods:

- **Electronic Mail**

E-mail relays your question to us quickly and allows us to respond, as soon as we have information for you. Send e-mail to [support@process.com](mailto:support@process.com). Be sure to include your:

- Name
- Telephone number
- Company name
- Process Software product name and version number
- Operating system name and version number

Describe the problem in as much detail as possible. You should receive an immediate automated response telling you that your call was logged.

- **Telephone**

If calling within the continental United States or Canada, call Process Software Technical Support toll-free at 1-800-394-8700. If calling from outside the continental United States or Canada, dial +1-508-628-5074. Please be ready to provide your name, company name, and telephone number.

- **World Wide Web**

There is a variety of useful technical information available on our World Wide Web home page, <http://www.process.com> (select **Support**).

## License Information

VAM includes a software license that entitles you to install and use it on one machine. Please read and understand the *Software License Agreement* before installing the product. If you want to use VAM on more than one machine, you need to purchase additional licenses. Contact Process Software or your distributor for details.

## Maintenance Services

Process Software offers a variety of software maintenance and support services. Contact us or your distributor for details about these services.

## Reader's Comments Page

The *VAM Administration and User's Guide* includes Reader's Comments as the last page. If you find an error in this guide or have any other comments about it, please let us know. Return a completed copy of the Reader's Comments page, or send e-mail to [techpubs@process.com](mailto:techpubs@process.com).

Please make your comments specific, including page references whenever possible. We would appreciate your comments about our documentation.

## Documentation Set

The documentation set for VAM consists of the following:

- ***Administration and User's Guide*** — For system managers, general users, and those installing the software. The guide provides installation and configuration instructions for the VAM products.
- ***Release Notes*** for the current version of VAM — For all users, system managers, and application programmers. The *Release Notes* are available online on your VAM media and are accessible before or after software installation.

## Conventions Used

| Convention                      | Meaning  |
|---------------------------------|--|
| host                            | Any computer system on the network. The local host is your computer. A remote host is any other computer.  |
| monospaced type                 | System output or user input. User input is in <b>bold type</b> .<br>Example: <code>Is this configuration correct? YES</code><br>Monospaced type also indicates user input where the case of the entry should be preserved.                                     |
| italic type                     | Variable value in commands and examples. For example, <i>username</i> indicates that you must substitute your actual username. Italic text also identifies documentation references.   |
| [ <i>directory</i> ]            | Directory name in an OpenVMS file specification. Include the brackets in the specification.  |
| [optional-text]                 | (Italicized text and square brackets) Enclosed information is optional. Do not include the brackets when entering the information.<br>Example: <code>START/IP line address [info]</code><br>This command indicates that the <i>info</i> parameter is optional. |
| { <i>value</i>   <i>value</i> } | Denotes that you should use only one of the given values. Do not include the braces or vertical bars when entering the value.  |
| <b>Note!</b>                    | Information that follows is particularly noteworthy.   |
| <b>CAUTION!</b>                 | Information that follows is critical in preventing a system interruption or security breach.   |
| <b>key</b>                      | Press the specified key on your keyboard.  |
| <b>Ctrl/key</b>                 | Press the control key and the other specified key simultaneously.  |
| <b>Return</b>                   | Press the Return or Enter key on your keyboard.  |



# Chapter 1

---

## Before You Begin

### Introduction

This chapter introduces you to and prepares you for the VMS Authentication Module (VAM) product installation, configuration, startup, and testing. It is for the OpenVMS system manager or technician responsible for product installation and configuration.

### Steps to Get VAM Up and Running

To get VAM up and working, you must perform the following steps:

**Table 1-1 Getting VAM Up and Running**

|          |                                |  |
|----------|--------------------------------|--|
| <b>1</b> | Load the license pack.         |  |
| <b>2</b> | Install the software.          | See Chapter 2, <i>Installing and Configuring VAM</i> |
| <b>3</b> | Configure the VAM environment. | See Chapter2, <i>Installing and Configuring VAM</i>  |

## Prepare for Installation

VAM installation involves using the VMSINSTAL procedure. Preparing for installation involves:

- Understanding the hardware and software requirements
- Determining if you have sufficient disk space and global pages for the installation
- Determining where to install the software

## Hardware Requirements

VAM has no special hardware requirements beyond those stated in the Software Product Description for TCPware, MultiNet or HP's TCP/IP Services.

## Software Requirements

VAM supports OpenVMS/VAX version 7.3; OpenVMS Alpha version 6.2, 7.0, 7.1, 7.2-1, 7.2-2, 7.3, 7.3-1, 7.3-2, 8.2, 8.3; OpenVMS I64 version 8.2, 8.2-1, 8.3; MultiNet version 4.4 or later, TCPware version 5.6-2 or later, UCX version 4.0 ECO 5 and later, and TCP/IP Services version 5.0 and later.

## Disk Space and Global Pages

The destination device for your VAM software must have enough disk space so that you can install and run the software. Your system will require approximately 20,000 free blocks to install VAM, and will require approximately 1,800 blocks net after installation.

## General Requirements

Check at this point that you:

- Have OPER, SYSPRV, or BYPASS privileges
- Can log in to the system manager's account
- Are the only user logged in (recommended)
- Backed up your system disk on a known, good, current, full backup (recommended)
- Need to reinstall VAM after performing a major VMS upgrade
- Ensure MultiNet, TCPware or TCP/IP Services (or UCX) is currently running.

## Where to Install VAM

Install VAM in a location depending on the following:

- Generally, on your system disk, but you can install VAM anywhere, just answer the question when it appears. This is also where you would keep your "common" files. Node-specific files should always be on your system disk.
- If the machine is in a single platform cluster, on a common disk.
- If the machine is in a mixed platform cluster, once on the Alpha system disk (or disks), once on

the I64 system disk (or disks), and once on the VAX common system disk.

## Release Notes and Online Documentation

The VAM *Release Notes* provide important information on the current release.

- The Release Notes is a text file which can be obtained in one of three ways:
  - By performing a partial installation
  - During the full installation
  - After the installation

To perform a partial installation (see Example 1-1):

**1** Invoke VMSINSTAL at the system prompt:

```
$ @SYS$UPDATE:VMSINSTAL VAM010 device OPTIONS N
```

The *device* is the mount location of the distribution volumes.

**2** Press **Return** at the prompt

```
Are you satisfied with the backup of your system disk [YES]?
```

**3** Select the option by number as to whether you want to display or print the *Release Notes*, or both.

**4** If you requested a printout, enter the queue name for the printer. The default is SYS\$PRINT.

**5** Press **Return** at the prompt

```
Do you want to continue the installation [NO]?:
```

```
This will print the VAM V1.0 Release Notes.      (Note that if you enter YES at the prompt,
you proceed with the full installation.)
```

**6** You see the message

```
Product's release notes have been moved to SYS$HELP.
```

**7** If you want to read or print the *Release Notes* after you exit the installation, you can access the VAM010.RELEASE\_NOTES files in the SYS\$HELP directory, as in:

```
$ TYPE SYS$HELP:VAM010.RELEASE_NOTES
```

**Note!** For this command to work as desired, do not redefine the SYS\$HELP directory logical.

### Example 1-1 Performing a Partial Installation to Obtain the Release Notes

```
$ @SYS$UPDATE:VMSINSTAL VAM010 DKA300: OPTIONS N          [1]
```

```
OpenVMS AXP Software Product Installation Procedure V7.1
```

```
It is 3-MARCH-2006 at 11:01.
```

```
Enter a question mark (?) at any time for help.
```

```
* Are you satisfied with the backup of your system disk [YES]? Return [2]
```

```
The following products will be processed:
```

```
VAM V1.0
```

## Before You Begin

---

Beginning installation of VAM V1.0 at 11:01

%VMSINSTAL-I-RESTORE, Restoring product save set A ...

Release notes included with this kit are always copied to SYS\$HELP.

Additional Release Notes Options:

1. Display release notes
2. Print release notes
3. Both 1 and 2
4. None of the above

\* Select option [2]: **Return** [3]

\* Queue name [SYS\$PRINT]: **Return** [4]

Job VAM010 (queue SYS\$PRINT, entry 1) started on SYS\$PRINT

\* Do you want to continue the installation [NO]? **Return** [5]

%VMSINSTAL-I-RELMOVED, Product's release notes have been moved to  
SYS\$HELP. [6]

VMSINSTAL procedure done at 11:02

.  
\$TYPE SYS\$HELP:VAM010.RELEASE\_NOTES [7]

# Installing and Configuring VAM

## Introduction

This chapter takes you through the VMS Authentication Manager (VAM) product installation procedure and certain post-installation tasks. It is for the OpenVMS system manager, administrator, or technician responsible for product installation.

To prepare for installation, see Chapter 1, *Before You Begin*.

**Note!** Once you have installed VAM, you need to reinstall it after you have done a major OpenVMS upgrade.

To install VAM:

- 1 Load the software.
- 2 Run the VMSINSTAL procedure.
- 3 Install other products, if needed, and perform post-installation tasks.

## Load the Software

VAM is downloaded from the Process Software FTP site. Information on downloading the software will be supplied to users by Process Software.

There are two steps to loading the VAM software:

- 1 Log in to the system manager's account.
- 2 Physically load the distribution media onto the appropriate device.
  - In a VMScluster environment, if you want to access the media from more than one node, enter the following:  

```
$ MOUNT/CLUSTER/SYSTEM device VAM010
```
  - On a standalone system, or if you want to prevent multiple users from accessing the software,

enter the following:

```
$ MOUNT device VAM010
```

**Note!** If you install VAM on a VMS cluster that has a common system disk, install the software on only one node in the cluster.

Be sure to configure VAM on all systems in a VMS cluster that has a common system disk, even though it only needs to be installed once.

## Start VMSINSTAL

VMSINSTAL is the OpenVMS installation program for layered products. VMSINSTAL prompts you for any information it needs. Table 2-1 shows the steps to follow.

**Table 2-1 Starting VMSINSTAL**

| Step | For this task...   | Enter this response...  |
|------|--|---|
| 1    | Make sure that you are logged in to the system manager's account, and invoke VMSINSTAL       | @SYSS\$UPDATE:VMSINSTAL   |
| 2    | Determine if you are satisfied with your system disk backup                                  | <b>Return</b> or <b>Y</b> (Yes) or <b>N</b> (No)                    |
| 3    | Determine where the distribution volumes will be mounted                                     | The disk (and directory) where you want the software to be mounted. |
| 4    | Enter the products you want processed from the first distribution volume set                 | <b>VAM010</b>   |
| 5    | Enter the installation options you wish to use (such as obtaining the <i>Release Notes</i> ) | <b>Return</b> for no options or <b>N</b> for <i>Release Notes</i> . |
| 6    | Specify the device where you want the files installed.                                       | <b>Return</b> if accepting default of SYSS\$SYSDEVICE:              |

## Sample Installation

```
$ @sys$update:vmsinstal vam010 dka600:
```

```
OpenVMS Software Product Installation Procedure V8.2
```

```
It is 16-FEB-2006 at 14:09.
```

Enter a question mark (?) at any time for help.

%VMSINSTAL-W-NOTSYSTEM, You are not logged in to the SYSTEM account.

%VMSINSTAL-W-ACTIVE, The following processes are still active:

DECW\$SERVER\_0

DECW\$TE\_043B

\* Do you want to continue anyway [NO]? y

\* Are you satisfied with the backup of your system disk [YES]?

The following products will be processed:

VAM V1.0

Beginning installation of VAM V1.0 at 14:09

%VMSINSTAL-I-RESTORE, Restoring product save set A ...

VMS Authentication Module (R)

ALL RIGHTS RESERVED UNDER THE COPYRIGHT LAWS OF THE UNITED STATES

This licensed material is the valuable property of Process Software. Its use, duplication, or disclosure is subject to the restrictions set forth in the License Agreement.

Other use, duplication or disclosure, unless expressly provided for in the license agreement, is unlawful.

\* What device do you want to install VMS Authentication Module on [SYS\$SYSDEVICE]:

\* Do you want to purge files replaced by this installation [YES]?

The installation will now proceed with no further questions.

\*\*\*\*\*

To complete this installation, you must refer to the documentation and the Release Notes for post-installation instructions.

\*\*\*\*\*

%VMSINSTAL-I-MOVEFILES, Files will now be moved to their target directories...

Installation of VAM V1.0 completed at 14:09

Adding history entry in VMI\$ROOT:[SYSUPD]VMSINSTAL.HISTORY

```
Creating installation data file: VMI$ROOT:[SYSUPD]VAM010.VMI_DATA
```

```
VMSINSTAL procedure done at 14:10
```

```
$
```

## Installing VAM for the First Time on a Common VMScluster System Disk

No special preparation is required after installing VAM on one node of a VMScluster with a common system disk.

## Installing VAM on Mixed Platform Clusters

VAM has no files which can be shared between cluster systems of different architectures.

## Post-Installation Steps

The SDCONF.REC file must be obtained from the ACE/Server system or from another VMS system running VAM. This file is to be copied to the `<install_device>:[VAM]` directory. This is a binary file, so it must be transferred via ftp in binary mode from a non-VMS system.

### ***Post-Installation Using the SecurID or Local UAF VAM Callable Module***

To use the VAM callable module, the system manager must add the line

```
@<install_device>:[VAM]VAM_STARTUP
```

to the SYSTARTUP\_VMS.COM file (SYSTARTUP\_V5.COM on VAX/VMS 5.5-2).

Beyond that, no further configuration on the client system is required.

The user will be responsible for using the provided VAM API to integrate VAM into the desired application(s).

### ***Post-Installation Using the SecurID VAM OpenVMS LOGINOUT Callouts***

The OpenVMS system requires further configuration to enable the LOGINOUT callouts.

First, the dynamic SYSGEN parameter LGI\_CALLOUTS must be set to "1":

Next, the system manager must determine which users are to be required to use SecurID. See chapter 4, *Using VAM*, for information on configuring the LGI callouts.

To use the VAM callable module, the system manager must add the line

@<install\_device>:[VAM]VAM\_STARTUP LGI

to the SYSTARTUP\_VMS.COM file (SYSTARTUP\_V5.COM on VAX/VMS 5.5-2).

**Note!** Including the LGI parameter on the VAM\_STARTUP command line will enable both the VAM LGI callouts and the VAM callable module.

### **Optional Post-Installation Steps**

The file <install-device>:[VAM]VAM\_SPECIFIC\_STARTUP.TEMPLATE may be edited and renamed to <install\_device>:[VAM]VAM\_SPECIFIC\_STARTUP.COM. The file contains system-or-site-specific commands to be executed when VAM starts.



## Chapter 3

---

# Using VAM

### Introduction

The VMS Authentication Module (VAM) provides users of OpenVMS systems controlled access to both user-written applications and the OpenVMS system overall using SecurID. It can be incorporated into an OpenVMS-based platform in two ways:

- Via an API that the user incorporates into a specific application to control access to that application
- On a system-wide basis via use of the LGI callouts for OpenVMS LOGINOUT.EXE.

This chapter describes the two mechanisms and how they are implemented.

### The VAM API

The API allows VAM to be incorporated into user-written applications to control access to those applications. The API allows authentication via SecurID tokens or via the local system UAF.

This can be used by a business that uses normal operating-system access for its internal functions, but which may need further controlled access to specific applications that interface to counterparts on remote systems. In this case, VAM provides an additional layer of security for access to that application.

The specific API calls are documented in chapter 4.

### The API Authentication Philosophy

The authentication process begins with the user calling the VMSAuthenticate function, providing the username for the user, the type of authentication to perform and callbacks necessary to carry on a further dialog if needed.

For SECURID processing, the authentication routines carry on the dialog with the RSA Authentication Manager, handling all the internal processing necessary. This includes the capability to handle replicated servers, etc..

For LOCALUAF processing, the authentication routines perform many of the same checks that the VMS LOGINOUT processing does in order to validate the user.

The authentication routines will not carry on the actual dialog with the user. The user program, by supplying the dialog callbacks, will be required to do the actual dialog, using prompts supplied by the authentication routines. In this way, the user may tailor this to the user's specific environment (video terminal, DECwindows application, etc).

When prompting for data via the dialog callbacks, the user is responsible for disabling terminal echo prior to reading the information, and re-enabling it after reading the information, and may be responsible (depending on the type of authentication being performed) for performing edits on the input data (such as being of proper length and type).

The basic processing will be as follows:

- The user is prompted for the username within the context of the user program.
- The user program calls `VMSAuthenticate()` to initialize processing. The first parameter to this function determines the authentication mechanism to use (`SECURID` or `LOCALUAF`).
- `VMSAuthenticate` may use the callback routines to obtain more information from the user or to display information to the user.
- `VMSAuthenticate` will return to the original caller with a status indicating whether the user has been authenticated.

## Controlling LOCALUAF Access to the Application

Some installations may have several applications protected via VAM and using LOCALUAF processing, but which they want to further restrict access to. For example, the company may want the PAYROLL application restricted to only people from the payroll department, while the INVENTORY application might be restricted to salespeople.

VAM provides a mechanism for restricting access in VAM-enabled applications by using VMS rights ids. When adding the VAM interface to an application, the application programmers may add the *identifier* field to the `VMSAuthenticate()` function call (see chapter 4, *Using the VAM API*, for information on calling `VMSAuthenticate`). VAM then attempts to match *identifier* with a rights id in the UAF record for the username specified in the call to `VMSAuthenticate`. If a match is made, access is allowed; otherwise, access is denied.

If *identifier* is not specified or is blank when calling `VMSAuthenticate`, then *identifier* will default to `VAM_UAF_ID`. Therefore, the `VAM_UAF_ID` rights id must be granted to all VAM users using LOCALUAF processing if *identifier* is not specified in the call to `VMSAuthenticate`.

**Note!** There is no equivalent functionality for use when performing SECURID processing. Access in that case is solely determined by the RSA Authentication Manager.

For example, ABC corporation has three VAM-enabled applications using LOCALUAF processing: payroll, inventory and personnel. User John Doe will be allowed to access only INVENTORY, while Jane Doe will be allowed to access PERSONNEL and PAYROLL. To set these accounts up, the following steps may be used:

```

$ run sys$system:authorize
UAF> add/identifier payroll
%UAF-I-RDBADDMMSG, identifier PAYROLL value %X80010003 added to rights
database
UAF> add/identifier inventory
%UAF-I-RDBADDMMSG, identifier INVENTORY value %X80010004 added to rights
database
UAF> add/identifier personnel
%UAF-I-RDBADDMMSG, identifier PERSONNEL value %X80010005 added to rights
database
UAF> grant/identifier inventory johndoe
%UAF-I-GRANTMSG, identifier INVENTORY granted to JOHNDOE
UAF> grant/identifier payroll janedoe
%UAF-I-GRANTMSG, identifier PAYROLL granted to JANEDOE
UAF> grant/identifier personnel janedoe
%UAF-I-GRANTMSG, identifier PERSONNEL granted to JANEDOE
UAF> Exit
%UAF-I-NOMODS, no modifications made to system authorization file
%UAF-I-NAFNOMODS, no modifications made to network proxy database
%UAF-I-RDBDONEMSG, rights database modified
$

```

Then, when adding VAM to, for example, the payroll application, the call to `VMSAuthenticate` would be:

```

status = VMSAuthenticate("LOCALUAF", username, 0, &IOCallback,
                        &InfoCallback, &TimeoutCallback,
                        &ScreenClearCallback, 0, "payroll", 0, 0);

```

## The VAM LGI Callouts

VAM may be incorporated into the OpenVMS login mechanism to control access to the entire system. VAM provides an OpenVMS shareable image, which the system manager can incorporate, using supported OpenVMS mechanisms, into the OpenVMS LOGINOUT mechanism. This image uses the SecurID protocols to supplement the standard OpenVMS login processing and provides the necessary user authentication to access the system as part of the login process.

**Note!** This section assumes the user has basic knowledge of how SecurID authentication works.

### Sample VAM Login

The following example shows a login to a system for a user that has not yet established a PIN

```

$ SET HOST VOODOO

Welcome to OpenVMS (TM) IA64 Operating System, Version V8.2-1

Username: johndoe
Enter PASSCODE:
You must select a new PIN.

```

```
Do you want the system to generate
your new PIN? (y/n) [n] n
Enter a new PIN between 4 and 8 alphanumeric
characters:
Re-enter new PIN to confirm:
PIN accepted. Wait for the tokencode to
change, then enter a new PASSCODE:

PASSCODE accepted.
```

```
Welcome to OpenVMS IA64 V8.2-1
```

```
Last interactive login on Monday, 23-JAN-2006 12:04:50.21
Last non-interactive login on Friday, 2-DEC-2005 07:33:34.74
```

```
You have 1 new Mail message.
```

```
VOODOO_$
```

### ***Controlling Access to the Callout***

The system manager configures the system to use the LGI callouts. This may be done in two ways:

- Define the logical name **VAM\_REQUIRE\_SECURID** system-wide. If defined, all users are required to use SecurID authentication.
- Add the rights identifier **VAM\_LGI\_SECURID** to the system rights database. This identifier may then be granted to those users that will be required to use SecurID authentication.

In addition, there are two logical names that, if defined, determine what types of terminal devices DECterm (FTAnn:) and/or DECnet CTERM (RTAnn:) devices are required log in using SecurID: The logicals may be defined to any value; the software simply uses the existence of the logicals to operate.

**VAM\_ALLOW\_DECNET\_LOGIN**

**VAM\_ALLOW\_DECTERM\_LOGIN**

**Note!** The system console (OPA0:) is never required to use SecurID processing, in order to prevent being locked-out of the system in the event of a network failure that prevents the VMS system from talking with the SecurID RSA Authentication Manager system(s).

**Note!** SSH logins are not affected by the VAM LGI callouts.

### **Other VAM-Specific Logical Names**

#### ***General Logicals***

These logical names are defined on all VAM systems. They are defined when the VAM\_STARTUP command procedure is executed.

**VAM**

This logical points to the `<install_device>:[VAM]` directory.

**VAM\_ROOT**

This logical points to `<install_device>:[VAM.]`. It may be used, for example, to specify the log file directory: `VAM_ROOT:[LOG]`.

**Logging Control Logicals**

The following logical names are used to affect logging for the VAM software. The logicals are located in the `VAM_SPECIFIC_STARTUP` command procedure and are normally commented out. This logging is used to debug VAM installations, and should generally be used only when recommended by Process Software.

**VAM\_LOGFILE**

This logical determines the location and name of the file used to log VAM transactions and errors.

**VAM\_CURRENT\_TRACE\_LEVEL**

This logical determines the level of detail in the VAM log. The level is a combination of the following bit masks:

`TRACE_EXECUTION (1)` - traces general steps the VAM module is performing.

`TRACE_EXECUTION_DEEP (2)` - verbose tracking of the VAM module processing.

`TRACE_INFO (4)` - Tracks informational messages generated by the VAM module

`TRACE_ERROR (8)` - Logs errors encountered by the VAM module

**RSATRACELEVEL**

This logical name is used to determine the level of detail in the SecurID logfile. This is a number from 1 to 65535, where 1 is the lowest level of tracing. This logical should never normally be defined, as it can have a severe impact on performance.

**RSATRACEDEST**

This logical defines the location and name of the SecurID log file. If this isn't defined, output will go to the user's terminal.

**SecurID Files Used by VAM**

The following files, used by SecurID processing, are found in the VAM directory. They should not normally be manipulated by the system manager:

**SDSTATUS.12**

This file is used by SecurID to keep track of the status of the RSA Authentication Manager servers and replicas. Each time a successful connection is made to a SecurID server, this file is rewritten.

**SECURID.**

This is the SecurID “node secret” file. It’s created after the first successful SecurID session.

## Chapter 4

---

# Using the VAM API

### Introduction

VAM provides an API for allowing user-written applications to use SecurID or local UAF authentication for controlling access to the application. This can be implemented by a business that uses normal operating-system access for its internal functions, but which may need further authentication for specific applications that interface to counterparts on remote systems. In this case, VAM provides an additional layer of security for access to that application.

This chapter describes how to use the VAM API when using VAM as a front-end for an application.

### Compiling a VAM Application

When compiling a source module that will call the VMSAuthenticate function, include the file VAM:VMSAUTHENTICATE.H.

### Linking A VAM Application

To link an application which uses the VAM API, include the file VAM:[VAM]VAM\_LINK.OPT. For example:

```
$ LINK MYAPPLICATION, VAM: [VAM]VAM_LINK.OPT /OPTION
```

### VAM API Functions

The following sections describe each of the VAM API calls. It includes not only the VMSAuthenticate function, but also the callback functions that are supplied by the user.

## VMSAuthenticate

The user application calls VMSAuthenticate to perform authentication. VMSAuthenticate must be supplied with an identifier that defines what type of authentication will take place and a username. A password may be supplied; however, it may be ignored (for example, in the case of performing SecurID authentication). The application must provide four callbacks to interact with the user.

VMSAuthenticate is a synchronous function; as such, it will not return until authentication completes successfully or fails.

### Format

```
int VMSAuthenticate {
    char *   AuthenticationType,
    char *   Username,
    char *   Password,
    int *    (*IOCallback)(),
    int *    (*InfoCallback)(),
    void *   (*TimeoutCallback)(),
    void *   (*ScreenClearCallback)(),
    int *    UserData,
    char *   Identifier,
    0, 0
};
```

### Inputs

- AuthenticationType - String (null-terminated) containing the type of authentication desired. Currently, must be "SECURID" or "LOCALUAF".
- Username - String (null-terminated) containing the username to be checked. The username is case-sensitive, and must match the case of the username when entered at the SecurID server.
- Password - String (null-terminated) containing the password to be checked. Ignored when AuthenticationType is "SECURID". Required when AuthenticationType is "LOCALUAF".
- IOCallback - Pointer to the user-defined callback to be called when a prompt/response dialog must be performed with the user.
- InfoCallback - Pointer to the user-defined callback to be called when an informational message must be displayed to the user.
- TimeoutCallback - Pointer to the user-defined callback to be called when a prompt timeout occurs.
- ScreenClearCallback - Pointer to the user-defined callback to be called when the screen is to be cleared after a prompt.
- UserData - Pointer to a user-defined data area. The contents and size of this data area are to be defined by the user, and may contain any context information desired by the user (for example, to identify the user or terminal being authenticated). This pointer will be passed to all user-defined callback routines.
- Identifier - String (null-terminated) that contains the name of the application. This will be used to match a VMS rights identifier when AuthenticationType is "LOCALUAF". If this field is

not specified for LOCALUAF processing, the identifier VAM\_UAF\_ID is used by default. This field is ignored for SECURID processing.

**Note!** The final two parameters (denoted by “0, 0” above) are reserved for future use but must be specified.

## Outputs

None.

## Returns

SS\$\_NORMAL

Authentication successful.

SS\$\_ABORT

Authentication was aborted by the server

SS\$\_BADPARAM

- No username was supplied
- Authentication type was not "SECURID" or "LOCALUAF"
- All callbacks were not supplied

SS\$\_CANCEL

- Authentication was aborted by the user

SS\$\_NOLICENSE

A valid license was not loaded.

**Note!** When performing authentication, the return status will never tell the user program (provided the arguments to the routine call were correct) why the authentication failed, only that it did fail. Providing this information to a user could provide an attacker with a clue as to what to try next.

## IOCallback

This user-application-supplied routine is called when a prompt/response dialog (consisting of exactly one prompt and expecting exactly one response) must be conducted with the user. The callback will be called with the information necessary to prompt for and return the required information (for example, the prompt to use, the length characteristics of the expected response, and if the response should be echoed to the terminal screen). The callback is expected to prompt for the data and return the null-terminated data in the response field. The callback is responsible (when directed by the EchoFlag) for turning echo to the terminal off before prompting for the data, and turning echo back on after getting the data from the caller.

In the case of performing SecurID authentication, the callback routine may perform any necessary editing to ensure the format & type of the data is correct (for example, to ensure it doesn't exceed the maximum length and is of the correct - numeric or alphanumeric - type). However, this isn't required, as the VMSauthenticate routine will also perform these checks on behalf of the user. The benefit of the user program performing these checks may lie in providing the ability to instantly provide feedback to the user in the event the response violates the input parameters.

### Format

```
int IOCallback(  
    char *    Prompt,  
    char *    Response,  
    int      MinRespLen,  
    int      MaxRespLen,  
    int      RespType,  
    int      EchoFlag,  
    int      Timeout,  
    int *    UserData  
);
```

### Inputs

- Prompt - String (null-terminated) that contains the prompt to display.
- MinRespLen - Minimum length of expected response.
- MaxRespLen - Maximum length of expected response.
- RespType - Type of data desired for the expected response, where 0 = numeric (0-9) and 1 = alphanumeric.
- EchoFlag - Set to 1 if the response should be echoed to the screen.
- Timeout - Time (in seconds) to display the prompt.
- UserData - Pointer to a user-defined data area. The contents and size of this data area are to be defined by the user, and may contain any context information desired by the user (for example, to identify the user or terminal being authenticated).

### Outputs

- Response - character string (null-terminated) that contains the response returned by the user.

## Returns

1 = successfully completed

0 = call was aborted. This will cause the authentication session to be terminated, with VMSAuthenticate returning a status of SSS\_CANCEL.

## InfoCallback

This user application-supplied callback routine is used when an informational message must be displayed by the user application with no response required (save for possibly an "OK" button in, for example, a DECwindows application).

### Format

```
int InfoCallback(  
    char *    Prompt,  
    int      Timeout,  
    Int *    UserData  
);
```

### Inputs

- Prompt - Character string (null-terminated) that contains the prompt to display.
- Timeout - Time (in seconds) to display the prompt
- UserData - Pointer to a user-defined data area. The contents and size of this data area are to be defined by the user, and may contain any context information desired by the user (for example, to identify the user or terminal being authenticated).

### Outputs

None.

### Returns

1 = successfully completed

0 = call was aborted. This will cause the authentication session to be terminated, with VMSAuthenticate() returning a status of SSS\_CANCEL.

## TimeoutCallback

This user application-supplied callback routine is invoked when a timeout for a prompt has been exceeded. The user application is required to terminate the I/O operation that it invoked. This timer is started just prior to calling the user-supplied IOCallback or InfoCallback routines, and the RSA Authentication Manager supplies its value.

**Note!** The user program must not disable AST's via the VMS \$SETAST system service. If this is done, timeouts won't be enforced.

### Format

```
void TimeoutCallback(  
    int * UserData  
);
```

### Inputs

UserData - Pointer to a user-defined data area. The contents and size of this data area are to be defined by the user, and may contain any context information desired by the user (for example, to identify the user or terminal being authenticated)..

### Outputs

None.

### Returns

None.

## ScreenClearCallback

This user application-supplied callback routine is used when the screen should be cleared subsequent to a call to IOCallback or InfoCallback.

### Format

```
int ScreenClearCallback(  
    int * UserData  
);
```

### Inputs

UserData - Pointer to a user-defined data area. The contents and size of this data area are to be defined by the user, and may contain any context information desired by the user (for example, to identify the user or terminal being authenticated).

### Outputs

None.

### Returns

None.

---

**A**

API  
LOCALUAF 3-2  
SECURID 3-1

---

**C**

conventions 1-ix  
customer support  
obtaining 1-vii

---

**D**

documentation set 1-viii

---

**E**

electronic mail 1-vii

---

**F**

File  
SDSTATUS.12 3-5  
SECURID. 3-5

---

**G**

general requirements 1-2  
global pages 1-2

---

**H**

hardware requirements 1-2

---

**I**

InfoCallback 4-6  
installation preparation 1-2  
installing on mixed platform clusters 2-4  
IOCallback 4-4

---

**L**

license information 1-vii  
load the software 2-1  
Logical  
RSATRACEDEST 3-5  
RSATRACELEVEL 3-5  
VAM 3-5  
VAM\_ALLOW\_DECNET\_LOGIN 3-4  
VAM\_ALLOW\_DECTERM\_LOGIN 3-4  
VAM\_CURRENT\_TRACE\_LEVEL 3-5  
VAM\_LOGFILE 3-5  
VAM\_REQUIRE\_SECURID 3-4  
VAM\_ROOT 3-5

---

**M**

maintenance services 1-vii

---

**O**

online help 1-vi

---

**R**

reader's comments 1-viii  
release notes 1-3  
required disk space 1-2

---

**S**

ScreenClearCallback 4-8  
software requirements 1-2  
starting VMSINSTAL 2-2

---

**T**

TCPware  
online documentation 1-3  
post-installation tasks 2-4  
telephone 1-vii  
TimeoutCallback 4-7  
Trace Level  
TRACE\_ERROR 3-5  
TRACE\_EXCUTION\_DEEP 3-5  
TRACE\_EXECUTION 3-5  
TRACE\_INFO 3-5

---

---

**V**

VAM public mailing list 1-vi  
VAM\_LGI\_SECUREID 3-4  
VMSSAuthenticate 4-2

---

**W**

where to install 1-2  
World Wide Web 1-vii

## Reader's Comments

### VMS Authentication Module Version 1.0 Administration and User's Guide

Your comments and suggestions will help us to improve the quality of our future documentation. Please note that this form is for comments on documentation only.

| <b>I rate this guide's:</b>                | <b>Excellent</b> | <b>Good</b> | <b>Fair</b> | <b>Poor</b> |
|--|------------------|-------------|-------------|-------------|
| Accuracy                                   | 0                | 0           | 0           | 0           |
| Completeness (enough information)          | 0                | 0           | 0           | 0           |
| Clarity (easy to understand)               | 0                | 0           | 0           | 0           |
| Organization (structure of subject matter) | 0                | 0           | 0           | 0           |
| Figures (useful)                           | 0                | 0           | 0           | 0           |
| Index (ability to find topic)              | 0                | 0           | 0           | 0           |
| Ease of use                                | 0                | 0           | 0           | 0           |

1. I would like to see more/less: \_\_\_\_\_
2. Does this guide provide the information you need to perform daily tasks? \_\_\_\_\_
3. What I like best about this guide: \_\_\_\_\_
4. What I like least about this guide: \_\_\_\_\_

My additional comments or suggestions for improving this guide: \_\_\_\_\_  
\_\_\_\_\_

I found the following errors in this guide:

| <b>Page</b> | <b>Description</b> |
|-------------|--------------------|
| _____       | _____              |
| _____       | _____              |

Please indicate the type of user/reader that you most nearly represent:

- |                        |                       |                        |                             |
|------------------------|-----------------------|------------------------|-----------------------------|
| System Manager         | <input type="radio"/> | Educator/Trainer       | <input type="radio"/>       |
| Experienced Programmer | <input type="radio"/> | Sales                  | <input type="radio"/>       |
| Novice Programmer      | <input type="radio"/> | Scientist/Engineer     | <input type="radio"/>       |
| Computer Operator      | <input type="radio"/> | Software Support       | <input type="radio"/>       |
| Administrative Support | <input type="radio"/> | Other (please specify) | <input type="radio"/> _____ |

Name: \_\_\_\_\_ Dept. \_\_\_\_\_  
Company: \_\_\_\_\_ Date \_\_\_\_\_  
Mailing Address: \_\_\_\_\_

After filling out this form, FAX or mail it to:  
**Process Software, 959 Concord Street, Framingham, MA 01701-4682**  
**Attention: Technical Publications Group FAX 508-879-0042 e-mail:techpubs@process.com**

