

# SSH FOR OPENVMS

version 2.4

OpenVMS Security Solution

## Complete SSH Solution for Alpha, VAX and Integrity Systems using HP TCP/IP Services

*SSH server and client provide secure encrypted communications over the Internet.*

### SECURE SHELL (SSH) PROTECTION

SSH for OpenVMS server and client software provides secure communications for system administrators using HP TCP/IP Services for OpenVMS on Alpha, VAX, or Integrity systems. It protects against a wide variety of potential security breaches such as spoofing, eavesdropping or hijacking a session, and man-in-the-middle attacks. System administrators can trust that user files, e-mails, and data reach their destination securely (see Figure 1).



SSH is the defacto standard for Internet security. SSH protocol version 2 is the basis for the Internet Engineering Task Force (IETF) SECSH standard. Many large enterprises and government organizations have used Process Software's SSH software worldwide on both MultiNet and TCPware TCP/IP stacks for OpenVMS for many years. The SSH2 server and client are compiled from unaltered cryptographic source which is FIPS 140-2 Level 2 compliant.

### AUTHENTICATION AND ENCRYPTION

SSH is a protocol that provides strong authentication and secure encrypted communications over unsecured channels. The more secure asymmetric cipher called Diffie-Hellman can be used for host authentication. Diffie-Hellman provides additional security by eliminating the need for exchanging private keys over the wire. It allows users the advantage of continually authenticating throughout the entire session. SSH for OpenVMS also supports a wide variety of strong encryption algorithms including IDEA, DES, 3DES, ARCFOUR, Blowfish, Twofish, AES-128, and CAST-128.

Managing SSH authentication is simplified with single sign-on support. SSH for OpenVMS works with existing PKI certificates and Kerberos infrastructure. A public-key server and assistant have been added to make it easier to manage keys for SSH public key authentication. The public-key subsystem and assistant can be used to add, remove, and list public keys stored on a remote server.

### SECURE APPLICATION TUNNELING

SSH for OpenVMS not only encrypts Telnet sessions, but many other applications with port forwarding. Any application can be encrypted that has a known port number. This includes e-mail, database connections, X-Windows, remote printing, and more. System administrators can choose which applications to encrypt based on their corporate security requirements, avoiding unnecessary network overhead. Also, data compression improves performance of slow network connections.

## Features

- Defacto standard for secure communications over the Internet
- Multi-protocol support: SSH protocol v1 and v2 server and client
- Provides secure file transfer with Secure Copy Protocol (SCP) and Secure File Transfer Protocol (SFTP) servers and clients
- Secures numerous applications with port forwarding
- Provides many authentication and encryption options
- Easy to manage using single sign-on
- Operates with most third-party SSH servers and clients
- Saves time and connection fees with data compression support
- Protects investment with support for HP TCP/IP Services for OpenVMS v4.0 or higher and OpenVMS v6.2 or higher on AXP, or OpenVMS v5.5-2 on VAX. Also supported is HP TCP/IP Services for OpenVMS v5.5 or higher and OpenVMS v8.2 or higher on Integrity

**PROCESS**<sup>TM</sup>  
SOFTWARE

A HALO TECHNOLOGY HOLDING COMPANY

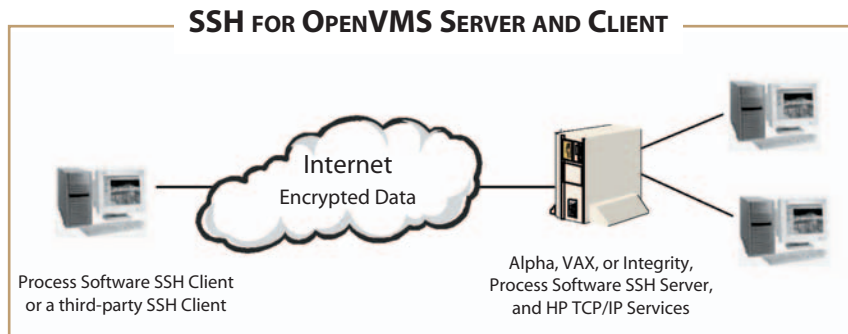


Figure 1

## SECURE DATA TRANSFERS

SSH for OpenVMS increases security with SFTP and SCP support. Both protocols allow SSH users to perform secure file transfers across an unsecured network. It provides system administrators with the ability to add, move, copy and delete files securely. SFTP and SCP utilize the SSH server and client as a basis for accomplishing this advanced level of security.

Both SFTP and SCP can be used to securely transfer files in ASCII, BINARY, or OpenVMS format when implementing SSH file transfer protocol v3 and v4. Support for this protocol improves file transfer interoperability between different operating systems.

## INTEROPERABILITY

The SSH for OpenVMS server and client are flexible, supporting a wide variety of third-party SSH servers and clients on the market today. This includes servers and clients on UNIX, Macintosh, Linux, and Windows platforms.

## ABOUT PROCESS SOFTWARE

Process Software is a premier supplier of communications software solutions to mission critical environments. With 20 years in business, we were early innovators of email software and anti-spam technology. Process Software has a proven track record of success with many Global 2000 and Fortune 1000 customers.

## PROCESS SOFTWARE'S TECHNICAL SERVICES PROGRAM

Process Software's Technical Services Program has a well-deserved reputation for excellence. Services include consulting, training, software maintenance, online resources, and standard or 24-hour support.

## PREREQUISITE SOFTWARE

SSH for OpenVMS requires HP TCP/IP Services for OpenVMS v4.0 (plus ECO 5) or higher, and one of the following: OpenVMS v6.2 or higher on Alpha, OpenVMS v5.5-2 or higher on VAX, or OpenVMS v8.2 or higher on Integrity systems. In order to enable Kerberos v5 authentication in the SSH server, the HP OpenVMS Kerberos v5 product must be installed (see <http://h71000.www7.hp.com/openvms/products/kerberos/>). This restricts support for Kerberos to OpenVMS Alpha v7.2-2 or higher.

## FREE EVALUATION SOFTWARE!

Please call 800-722-7770 or email [sales@process.com](mailto:sales@process.com) to get your free evaluation copy of SSH for OpenVMS.

## SSH at a Glance

### SERVER AND CLIENT

SSH protocol v1 and v2 server and client  
SFTP v3 and v4 server and client  
SSH server supports most third-party SSH clients on many platforms  
SSH v2 server and client are compiled from an unaltered source which is FIPS 140-2 Level 2 compliant

### AUTHENTICATION AND ENCRYPTION

Host authentication options: Public Key, Private Key, and Diffie-Hellman  
Client authentication options: password, Rhosts, Rhosts with RSA host Authentication, RSA Challenge-Response, and Public Key  
RSA and DSA Public Key  
Signatures: SHA-1 Message Integrity  
Encryption Ciphers: IDEA, DES, 3DES, ARCFOUR, Blowfish, Twofish, AES-128, and CAST-128  
SSH single sign-on with support for Kerberos v5 and PKI certificates  
Public-Key Subsystem and Assistant  
CERTTOOL utility for X.509 certificate management  
Single sign-on access to LDAP and RSA SecurID authentication when used with VAM

### APPLICATIONS

Replaces Telnet, rlogin, rsh, FTP and rcp  
Port Forwarding encrypts third-party applications  
X-11 Forwarding encrypts X-11 display

### OTHER

SSH v2 IETF Internet standard  
Data compression  
Runs on Alpha, VAX, and Integrity systems

Process Software  
959 Concord Street  
Framingham, MA 01701

Telephone:  
U.S./Canada (800)722-7770  
International(508)879-6994

Fax: (508)879-0042

Web: [www.process.com](http://www.process.com)

Email: [info@process.com](mailto:info@process.com)