

How to Configure SSH Public-Key Based Authentication for TCPIP V5.7 SSH/SSH.COM on OpenVMS

Table of contents

1. How to Configure SSH Public-Key Based Authentication for TCP/IP V5.7 SSH/SSH.COM on OpenVMS	3
2. Procedure	4
2.1 Configure the SSH Client	4
2.2 Configure the SSH Server	6
2.3 Test the Configuration	8

1. How to Configure SSH Public-Key Based Authentication for TCP/IP V5.7 SSH/SSH.COM on OpenVMS

Applies to: TCP/IP Services for OpenVMS V5.7

Public key authentication uses a private/public key pair to verify a user's identity. The private key remains on the client system, while the public key is stored on the server.

This article describes how to configure both the client and server side. After configuration, SSH, SFTP, and SCP connections can authenticate using the key pair instead of a password.

Example Environment

- Client host: SSH-CLIENT_HOSTNAME.DOMAIN.COM
- Server host: SSH-SERVER_HOSTNAME.DOMAIN.COM
- Username: SMITH
- User directory: DKA0:[SMITH]

The SSH key filename used throughout this article is *key_filename*. You may choose any meaningful name for your key pair. For easier administration, use a unique and descriptive name that identifies the key owner, system, or purpose.

2. Procedure

2.1 Configure the SSH Client

1. Enable the SSH Client.

Run the TCP/IP Services configuration utility:

```
$ @SYS$STARTUP:TCPIP$CONFIG.COM
```

From the available options, select Client components, then SSH Client, and then Enable & Start service on this node.

2. Confirm that Public Key Authentication is allowed.

Public key authentication is enabled by default. However, if the AllowedAuthentications setting has been modified, you may need to explicitly include publickey in the list of permitted authentication methods.

For example:

```
$ EDIT TCPIP$SSH_DEVICE:[TCPIP$SSH.SSH2]SSH2_CONFIG
AllowedAuthentications publickey
```

3. Generate a Key Pair.

Create an SSH directory if needed:

```
$ CREATE/DIRECTORY DKA0:[SMITH.SSH2]
```

Generate the key:

```
$ @SYS$MANAGER:TCPIP$DEFINE_COMMANDS.COM
$ SET DEFAULT DKA0:[SMITH.SSH2]
$ ssh_keygen key_filename
```

The utility prompts for a passphrase twice. Enter a passphrase for additional security, or leave it blank for batch or automated use.

A private key and public key (KEY_FILENAME.PUB) are created.

Protect the files as follows:

```
SET FILE/PROTECTION=(S,W,G,O:RWED) KEY_FILENAME.*
```

4. Create the IDENTIFICATION file and add the private key name.

```
$ CREATE DKA0:[SMITH.SSH2]IDENTIFICATION  
  
IdKey key_filename
```

Note: Do not include a file version such as ;1.

5. Transfer the Public Key to the server.

Use SFTP:

```
sftp user@server  
cd ssh2  
put KEY_FILENAME.PUB
```

Note: If the SSH server has not yet been enabled, skip this step and return to it after the server configuration is complete.

2.2 Configure the SSH Server

1. Enable the SSH Server.

Run the TCP/IP Services configuration utility:

```
$ @SYS$STARTUP:TCPIP$CONFIG.COM
```

From the available options, select Server components, then SSH, and then Enable & Start service on this node.

A server host key is created if one does not already exist.

2. Confirm Public Key Authentication is Allowed.

Public key authentication is enabled by default. However, if the AllowedAuthentications setting has been modified, you may need to explicitly include publickey in the list of permitted authentication methods.

For example:

```
$ TCPIP$SSH_DEVICE:[TCPIP$SSH.SSH2]SSHD2_CONFIG
$ AllowedAuthentications publickey
```

3. Verify the Public Key.

Ensure the user's SSH directory exists and the public key has been copied from the client.

Verify the key:

```
$ @SYS$MANAGER:TCPIP$DEFINE_COMMANDS.COM
$ SET DEFAULT DKA0:[SMITH.SSH2]
$ ssh_keygen -"F" key_filename.pub
```

A fingerprint should be returned. If no fingerprint is displayed, the key is not usable.

If the key originated from OpenSSH, convert it to SSH.COM format before use.

```
$ ssh-keygen -e -f openssh_key.pub > key_filename.pub
```

4. Set File Protection.

Protect the public key file:

```
$ SET FILE/PROTECTION=(S,W,G,O:RWED) key_filename.pub
```

5. Create the AUTHORIZATION File.

```
$ CREATE DKB0:[SMITH.SSH2]AUTHORIZATION.
```

Each entry consists of a single line containing the public key filename, for example:

```
KEY key_filename.pub
```

Note: Do not include a file version such as ;1.

2.3 Test the Configuration

The following examples demonstrate successful SSH and SFTP connectivity to the OpenVMS server.

SSH login

```
$ ssh user@server

Welcome to OpenVMS (TM) Alpha Operating System, Version V7.3-2
Unauthorized access is prohibited!

Authentication successful.
```

SSH Remote Command Execution

```
$ ssh user@server mc sysgen show scsnode

Welcome to OpenVMS (TM) Alpha Operating System, Version V7.3-2
Unauthorized access is prohibited!

Authentication successful.
```

Parameter Name	Current	Default	Min.	Max.	Unit	Dynamic
SCSNODE	"server"	" "	" "	"ZZZZ"	Ascii	

SFTP Connection

```
$ sftp user@server

Welcome to OpenVMS (TM) Alpha Operating System, Version V7.3-2
Unauthorized access is prohibited!

Authentication successful.
```