

# Public/Private Key Pairs

## Category: Security & Logging In

Public-key authentication is a means of identifying yourself by proving that you know the private key associated with a given public key. This method is more secure than password authentication, but it requires more effort to set up.

### Public-Key Basics

To use this method, you use the `ssh-keygen` program to generate a public/private key pair on your local system. You will be prompted for a passphrase which is used to encrypt the private key. By default, the private key is stored in `~/.ssh/id_rsa` and the public key is stored in `~/.ssh/id_rsa.pub`.

The private key should only be kept on your local system and should be encrypted using a passphrase that is at least as strong as any password you would normally use. The security of this method depends on keeping the private key safe and secure.

The public key can be safely copied to other systems and appended to `~/.ssh/authorized_keys` on those systems. The server uses this copy of the public key to confirm that you possess the private key.

When you authenticate to a server using public-key authentication, the SSH client offers a copy of the public key to the server and the server then compares it against the keys listed in your `~/.ssh/authorized_keys` file. If it matches, the server indicates that it is able to proceed with the authentication. At that point, the SSH client will prompt you for the passphrase in order to decrypt the private key. The private key is then used to sign a message that includes data specific to the SSH session. The server can then use its copy of the public key to verify the signature.

If the server can verify the signature, you are authenticated.

### Why Are Public/Private Keys More Secure Than Passwords?

- The passphrase is never sent over the network
- The private key is never sent over the network
- It is extremely computationally expensive to derive the private key from the public key
- Protects against man-in-the-middle attacks

---

Article ID: 33

Last updated: 13 Jul, 2012

The HEC Environment -> Security & Logging In -> Public/Private Key Pairs

<http://www.nas.nasa.gov/hecc/support/kb/entry/33/?ajax=1>