NAME

puttygen - public-key generator for the PuTTY tools

SYNOPSIS

puttygen (*keyfile* | **−t** *keytype* [**−b** *bits*])
[**−C** *new−comment*] [**−P**] [**−q**]
[**−O** *output−type* | **−l** | **−L** | **−p**]
[**−o** *output−file*]

DESCRIPTION

puttygen is a tool to generate and manipulate SSH public and private key pairs. It is part of the PuTTY suite, although it can also interoperate with the key formats used by some other SSH clients.

When you run **puttygen**, it does three things. Firstly, it either loads an existing key file (if you specified *keyfile*), or generates a new key (if you specified *keytype*). Then, it optionally makes modifications to the key (changing the comment and/or the passphrase); finally, it outputs the key, or some information about the key, to a file.

All three of these phases are controlled by the options described in the following section.

OPTIONS

In the first phase, **puttygen** either loads or generates a key. Note that generating a key requires random data, which can cause **puttygen** to pause, possibly for some time if your system does not have much randomness available.

The options to control this phase are:

keyfile Specify a key file to be loaded.

Usually this will be a private key, which can be in the (de facto standard) SSH-1 key format, or in PuTTY's SSH-2 key format, or in either of the SSH-2 private key formats used by OpenSSH and ssh.com's implementation.

You can also specify a file containing only a *public* key here. The operations you can do are limited to outputting another public key format or a fingerprint. Public keys can be in RFC 4716 or OpenSSH format, or the standard SSH-1 format.

−t *keytype*
Specify a type of key to generate. The acceptable values here are **rsa**, **dsa**, **ecdsa**, and **ed25519** (to generate SSH-2 keys), and **rsa1** (to generate SSH-1 keys).

−b *bits* Specify the size of the key to generate, in bits. Default is 2048.

−q Suppress the progress display when generating a new key.

−−old−passphrase *file*
Specify a file name; the first line will be read from this file (removing any trailing newline) and used as the old passphrase. **CAUTION:** If the passphrase is important, the file should be stored on a temporary filesystem or else securely erased after use.

−−random−device *device*
Specify device to read entropy from. By default, **puttygen** uses **/dev/urandom**, falling back to **/dev/random** if it has to.

In the second phase, **puttygen** optionally alters properties of the key it has loaded or generated. The options to control this are:

−C *new−comment*
Specify a comment string to describe the key. This comment string will be used by PuTTY to identify the key to you (when asking you to enter the passphrase, for example, so that you know which passphrase to type).

−P Indicate that you want to change the key's passphrase. This is automatic when you are generating a new key, but not when you are modifying an existing key.

In the third phase, **puttygen** saves the key or information about it. The options to control this are:

−O *output−type*
Specify the type of output you want **puttygen** to produce. Acceptable options are:

private Save the private key in a format usable by PuTTY. This will either be the standard SSH-1 key format, or PuTTY's own SSH-2 key format.

public Save the public key only. For SSH-1 keys, the standard public key format will be used ('**1024 37 5698745**...'). For SSH-2 keys, the public key will be output in the format specified by RFC 4716, which is a multi-line text file beginning with the line '**---- BEGIN SSH2 PUBLIC KEY ----**'.

public-openssh
Save the public key only, in a format usable by OpenSSH. For SSH-1 keys, this output format behaves identically to **public**. For SSH-2 keys, the public key will be output in the OpenSSH format, which is a single line ('**ssh-rsa AAAAB3NzaC1yc2**...').

fingerprint
Print the fingerprint of the public key. All fingerprinting algorithms are believed compatible with OpenSSH.

private-openssh
Save an SSH-2 private key in OpenSSH's format, using the oldest format available to maximise backward compatibility. This option is not permitted for SSH-1 keys.

private-openssh-new
As **private-openssh**, except that it forces the use of OpenSSH's newer format even for RSA, DSA, and ECDSA keys.

private-sshcom
Save an SSH-2 private key in ssh.com's format. This option is not permitted for SSH-1 keys.

If no output type is specified, the default is **private**.

−o *output−file*
Specify the file where **puttygen** should write its output. If this option is not specified, **puttygen** will assume you want to overwrite the original file if the input and output file types are the same (changing a comment or passphrase), and will assume you want to output to stdout if you are asking for a public key or fingerprint. Otherwise, the **−o** option is required.

−l Synonym for '**-O fingerprint**'.

−L Synonym for '**-O public-openssh**'.

−p Synonym for '**-O public**'.

−−new−passphrase *file*
Specify a file name; the first line will be read from this file (removing any trailing newline) and used as the new passphrase. If the file is empty then the saved key will be unencrypted. **CAUTION:** If the passphrase is important, the file should be stored on a temporary filesystem or else securely erased after use.

The following options do not run PuTTYgen as normal, but print informational messages and then quit:

−h, **−−help**
Display a message summarizing the available options.

−V, **−−version**
Display the version of PuTTYgen.

−−pgpfp
Display the fingerprints of the PuTTY PGP Master Keys, to aid in verifying new files released by the PuTTY team.

EXAMPLES

To generate an SSH-2 RSA key pair and save it in PuTTY's own format (you will be prompted for the passphrase):

puttygen −t rsa −C "my home key" −o mykey.ppk

To generate a larger (4096-bit) key:

puttygen −t rsa −b 4096 −C "my home key" −o mykey.ppk

To change the passphrase on a key (you will be prompted for the old and new passphrases):

puttygen −P mykey.ppk

To change the comment on a key:

puttygen −C "new comment" mykey.ppk

To convert a key into OpenSSH's private key format:

puttygen mykey.ppk −O private−openssh −o my−openssh−key

To convert a key *from* another format (**puttygen** will automatically detect the input key type):

puttygen my−ssh.com−key −o mykey.ppk

To display the fingerprint of a key (some key types require a passphrase to extract even this much information):

puttygen −l mykey.ppk

To add the OpenSSH-format public half of a key to your authorised keys file:

puttygen −L mykey.ppk >> $HOME/.ssh/authorized_keys