ssh-add(1)

NAME

ssh-add- add RSA or DSA identities for the authentication agent

SYNOPSIS

`ssh-add` [**`-lLdD`**] [*file* ...]

DESCRIPTION

The `ssh-add` utility adds RSA or DSA identities to the authentication agent, ssh-agent(1). When run without arguments, it attempts to add all of the files `$HOME/.ssh/identity` (RSA v1), `$HOME/.ssh/id_rsa` (RSA v2), and `$HOME/.ssh/id_dsa` (DSA v2) that exist. If more than one of the private keys exists, an attempt to decrypt each with the same passphrase will be made before reprompting for a different passphrase. The passphrase is read from the user's tty or by running the program defined in `SSH_ASKPASS` (see below).

The authentication agent must be running.

OPTIONS

The following options are supported:

`-d`

Instead of adding the identity, this option **removes** the identity from the agent.

`-D`

Deletes all identities from the agent.

`-l`

Lists fingerprints of all identities currently represented by the agent.

`-L`

Lists public key parameters of all identities currently represented by the agent.

ENVIRONMENT VARIABLES

`DISPLAY`
`SSH_ASKPASS`

If `ssh-add` needs a passphrase, it will read the passphrase from the current terminal if it was run from a terminal. If `ssh-add` does not have a terminal associated with it but `DISPLAY` and `SSH_ASKPASS` are set, it will execute the program specified by `SSH_ASKPASS` and open an X11 window to read the passphrase. This is particularly useful when calling `ssh-add` from a .Xsession or related script.

EXIT STATUS

The following exit values are returned:

`0`

Successful completion.

`1`

An error occurred.

FILES

These files should not be readable by anyone but the user. Notice that `ssh-add` ignores a file if it is accessible by others. It is possible to specify a passphrase when generating the key; that passphrase will be used to encrypt the private part of this file.

If these files are stored on a network file system it is assumed that either the protection provided in the file themselves or the transport layer of the network file system provides sufficient protection for the site policy. If this is not the case, then it is recommended the key files are stored on removable media or locally on the relevant hosts.

Recommended names for the DSA and RSA key files:

`$HOME/.ssh/identity`

> Contains the RSA authentication identity of the user for protocol version 1.

`$HOME/.ssh/identity.pub`

> Contains the public part of the RSA authentication identity of the user for protocol version 1.

`$HOME/.ssh/id_dsa`

> Contains the private DSA authentication identity of the user.

`$HOME/.ssh/id_dsa.pub`

> Contains the public part of the DSA authentication identity of the user.

`$HOME/.ssh/id_rsa`

> Contains the private RSA authentication identity of the user.

`$HOME/.ssh/id_rsa.pub`

> Contains the public part of the RSA authentication identity of the user.

ATTRIBUTES

See attributes(5) for descriptions of the following attributes:

ATTRIBUTE TYPE	ATTRIBUTE VALUE
Availability	SUNWsshu

SEE ALSO

ssh(1), ssh-agent(1), ssh-keygen(1), sshd(1M), attributes(5)

To view license terms, attribution, and copyright for OpenSSH, the default path is `/var/sadm/pkg/SUNWsshdr/install/copyright`. If the Solaris operating environment has been installed anywhere other than the default, modify the given path to access the file at the installed location.

AUTHORS

OpenSSH is a derivative of the original and free `ssh` 1.2.12 release by Tatu Ylonen. Aaron Campbell, Bob Beck, Markus Friedl, Niels Provos, Theo de Raadt and Dug Song removed many bugs, added newer features and created Open SSH. Markus Friedl contributed the support for SSH protocol versions 1.4 and 2.0.