NAME

ssh-keysign — ssh helper program for host-based authentication

SYNOPSIS

ssh-keysign

DESCRIPTION

ssh-keysign is used by ssh(1) to access the local host keys and generate the digital signature required during host-based authentication.

ssh-keysign is disabled by default and can only be enabled in the global client configuration file /etc/ssh/ssh_config by setting **EnableSSHKeysign** to "yes".

ssh-keysign is not intended to be invoked by the user, but from ssh(1). See ssh(1) and sshd(8) for more information about host-based authentication.

FILES

/etc/ssh/ssh_config
: Controls whether **ssh-keysign** is enabled.

/etc/ssh/ssh_host_dsa_key
/etc/ssh/ssh_host_ecdsa_key
/etc/ssh/ssh_host_ed25519_key
/etc/ssh/ssh_host_rsa_key
: These files contain the private parts of the host keys used to generate the digital signature. They should be owned by root, readable only by root, and not accessible to others. Since they are readable only by root, **ssh-keysign** must be set-uid root if host-based authentication is used.

/etc/ssh/ssh_host_dsa_key-cert.pub
/etc/ssh/ssh_host_ecdsa_key-cert.pub
/etc/ssh/ssh_host_ed25519_key-cert.pub
/etc/ssh/ssh_host_rsa_key-cert.pub
: If these files exist they are assumed to contain public certificate information corresponding with the private keys above.

SEE ALSO

ssh(1), ssh-keygen(1), ssh_config(5), sshd(8)

HISTORY

ssh-keysign first appeared in OpenBSD 3.2.

AUTHORS

Markus Friedl <markus@openbsd.org>