SSH CA helper

2021-05-16 09:11

Contents

1 Abstract

This is a sketch of an idea for a little command line tool for managing SSH CA keys and making certificates.

2 SSH CA

An SSH CA is an SSH key used to certify host and user keys. When a host key is certificate, each user can configure their SSH client to trust a host certificated made with a known CA key. They then only ever need to verify that the CA key is valid, rather than every new host key. The host certificate can specify the host name that it's valid for.

Similarly, a sysadmin can configure their SSH server to trust user certificate made with a CA key. The user certificate specifies which user account on the server it's valid for. This means the user doesn't need to have a password so they can log in once to add their SSH public key to their `authorized_keys` file on the server.

3 `sshca` the command line tool

`sshca` is a command line tool for managing SSH CA keys and making certificates. It's a wrapper around the `ssh-keygen` tool that aims to be easier to use and harder to misuse.

Each certificate has an automatically chosen serial number. `sshca` keeps track of the serial numbers that have been used.

Certificates can optionally have a validity period (valid from a time, and until a time). The period may be open ended.

3.1 Generate an SSH CA key

To generate a new SSH CA key pair and give is a short name:

```
$ sshca generate NAME
```

The key pair will be stored in `~/.ssh/sshca` and will by default be of type `ed25519` (elliptic curve), for higher security and smaller key size. The type can be specified with an option.

3.2 List existing SSH CA keys

To list SSH CA keys:

```
$ sshca list
default ed25519 ....
```

This lists all the keys in the `~/.ssh/sshca` directory.

3.3 Removing an SSH CA key

To remove an SSH CA key:

```
$ sshca remove-key NAME
```

This removes the named key from the `~/.ssh/sshca` directory.

3.4 Create a host certificate

To create a host certificate:

```
$ sshca cert-host KEYNAME HOSTPUB HOSTNAME > FILENAME
```

This create a host certificate using a named SSH CA key, for a given host public key, and ties it a given host name. The certificate is written to the standard output, and can be redirected to a file as usual on the command line.

3.5 Create a user certificate

To create a user certificate:

```
$ ssh ca cert-user KEYNAME USERPUB USERNAME > FILENAME
```

Similar to a host certificate, but for a user.