SSH client end setup for certificates

How to set up a client computer to use SSH certificates for host and client authentication.

Host Authenticattion:

ssh will recognize host certificates from any host whose certificate is signed by an authority identified in the file /etc/ssh/ssh_known_hosts.

To configure this you need the following line in /etc/ssh/ssh_config:

```
GlobalKnownHostsFile /etc/ssh/ssh_known_hosts
```

Then you need to append a line like the one below to /ets/ssh/ssh_known_hosts:

```
cat <<EOF | sudo tee -a /etc/ssh/ssh_known_hosts
@cert-authority * ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQDTcMC1gp\
Ey/r0E/nolRkiOH/ppenhnbj1BFHKRi/RdxttVWSHoMg9ilKADdz6nItm2HuEZ04\
tfIIbEs9yH4VdnWbfAbgfkZBHzY4rueXuo7xlnAWx14JMFuCT2WaVRmi6Sf8eUDP\
BB3sGjE2yPWSaQUDp6kMx1V8whES0jiW7CLDOSlU6fW0T6lLgaRZ9h49Rh3jcV3I\
5ZZg1ogD0YNKgjdgnzHuFeGAZCB5fI5L+ndC8KXTKmC7shYN1adSIoWS3XgQiUHm\
ajpwFEIYOBE6/xI8QFU/F44j5EjFvfPq1k9zPEvi0SKV68Rl8JZ0X/SontVRQ/To\
gvYvftDWt32jACdv3vUk+QDpyyym+R7SCOKX/STlT3FDk/yrHMHQBzYO1KKhnVFv\
KzzZs0umsqDSGrYSLialPUJ+ZuXDTSelov+P5s200ZBAPjxYD6YIGiBsPKgHssVQ\
7GUlz1mxgOObQNVQjbrgdGwpdnYpY4YlsogtybI1QIbDtU/fIRPHHeWWBOW+iZ1w\
9/XHnSyP0EFyzk+bYz21lRxJHLBsfWehshM3Mwqs+A3cmwzUyGQCeT8XV+mKe7y1\
VAiqVVQQjhjHCoU+N4XkdM8pUzR0NkC33amlV68e1EDSD0XAtLZCUrJfil18X9/R\
hWkiDVElMOPwmsp3nJ9jU3UQRQ7Yf97V3oLw== pbz@ogopogo.biz_hostca_bzhosts
EOF
```

The above authority currently authenticates the following hosts:

Authority: pbz@ogopogo.biz (tag bzhosts)

- mamey.ogopogo.biz
- repo.ogopogo.biz
- guanabana.bernatchez.net
- relay.bernatchez.net
- relay.ogopogo.biz
- repo.bernatchez.net

Client Authentication:

Generate a private/public key pair with this command:

```
/usr/bin/ssh-keygen -b 4096 -t rsa -C hostname_purpose -f hostname_purpose
```

Substitute ‘hostname’ above with a name for the client computer and ‘purpose’ with something indicating what the key will be used for. Something like this:

```
ssh-keygen -b 4096 -t rsa -C lancelaptop_jobberuser -f lancelaptop_jobberuser
```

Send an email to the signing authority requesting a signed certificate. Attach the public key generated above to the email. The certificate authority will attach a certificate granting you access in a return email. Put that certificate in the same directory where you store the private key.

When you load the private key into your ssh agent, the certificate will also be loaded.

Example:

```
ssh-add lancelaptop_jobberuser
```

You will need to respond with correct passphrase for your key and will get something like the following:

> Enter passphrase for lancelaptop_jobberuser:
>
> Identity added: lancelaptop_jobberuser (lancelaptop_jobberuser) Certificate added: lancelaptop_jobberuser-cert.pub (lancelaptop_jobberuser)

ISSUE:

> On ubuntu the ssh-add utility fails to load certificate files. This does not occur when the ssh-agent is the real ssh-agent, it occurs when the agent is the one implemented by gnome-keyring. The fix is to stop using the ssh component of gnome-keyring. Since the initialization process actually starts up a true ssh-agent and then launches gnome-keyring-ssh.desktop which clobbers AUTH_SOCKET to take it over, we revert back to the original ssh-agent by disabling gnome-keyring-ssh.desktop.

Disable gnome-keyring-ssh.desktop:

```
cd /etc/xdg/autostart/
sudo emacs gnome-keyring-ssh.desktop
```

Add the following line to the desktop file and save it

```
X-GNOME-Autostart-enabled=false
```

Then reboot