gnupg

Messages encrypted with your public key can be sent securely to you.
Two machines: centos-1 and centos-2

1. generate key (centos-1)
2. distribute key (centos-1)
3. import key (centos-2)
4. encrypt (centos-2)
5. decrypt (centos-1)

1. generate key
#generate

```
gpg --gen-key
```

(*enter your name, email and passphrase*)
#export the key to a file

```
gpg --export peter@uadmin.nl > peter.pub
```

2. distribute key
#share the key with others

```
scp peter.pub root@centos-2:/tmp
```

3. import key
#on the other server
#import the key

```
cd /tmp
gpg --import peter.pub
gpg --list-keys
```

4. encrypt
#create a message and encrypt it

```
echo hello > greetings
gpg --out greetings.secure --recipient peter@uadmin.nl --encrypt greetings
```

#send the message to the owner of the key

```
scp greetings.secure root@centos-1:/tmp
```

5. decrypt message
#on centos-1

```
cd /tmp
gpg --out received_message --decrypt greetings.secure
cat received_message
```