WBS 2.3.2 RACD Software Signatures

Background

Software distributed thru XSEDE repositories must be signed so that consumers can verify the source.

This page documents how to sign software packages.

XSEDE developer signature

Every developer placing packages in the development repository must sign them with a personal signing (ONLY) key pair created as shown below. Keys must be 2048 or 4096 bits long (4096 recommended), expire in 2 years or less (730 days), and use a SHA2 (SHA256 recommended) digest.

Begin by placing the following in your .gnupg/gpg.conf:

```
personal-digest-preferences SHA256
cert-digest-algo SHA256
default-preference-list SHA256 SHA512 SHA384 SHA224 AES256 AES192 AES CAST5 ZLIB BZIP2 ZIP
Uncompres
sed
```

Then generate your key as follows:

```
$ gpg --gen-key
...
Please select what kind of key you want:
   (1) DSA and Elgamal (default)
   (2) DSA (sign only)
   (5) RSA (sign only)
Your selection? 5
RSA keys may be between 1024 and 4096 bits long.
What keysize do you want? (2048) 4096
Requested keysize is 4096 bits
Please specify how long the key should be valid.
         0 = key does not expire
      <n>  = key expires in n days
      <n>w = key expires in n weeks
      <n>m = key expires in n months
      <n>y = key expires in n years
Key is valid for? (0) 730
Key does not expire at all
Is this correct? (y/N) y

You need a user ID to identify your key; the software constructs the user ID
from the Real Name, Comment and Email Address in this form:
    "Heinrich Heine (Der Dichter) <heinrichh@duesseldorf.de>"

Real name: **ENTER YOUR FIRST AND LAST NAME**
Email address: **ENTER YOU E-MAIL ADDRESS**
Comment:
You selected this USER-ID:
    "YOUR NAME <YOUR E-MAIL>"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? O
```

Publish it to the GPG server:

```
gpg --send-keys <key_id>
```

Send your phone number and the output of this command:

```
gpg --list-keys --fingerprint <key_id>
```

to XSEDE repository administrators thru an XSEDE ticket. Once the administrators have verified that your request is from you they will add you key to the list of XSEDE recognized developers so that others can verify that you produced the package.

How to sign RPMs

```
rpm --add-sign <package>.rpm
```

How to sign TARs

```
gpg --output <package>.sig --detach-sig <package>.{tar,tgz}
```

Signature Creation

The following process was used to generate XSEDE's software signature:

```
[xsedesig@software ~]$ gpg --gen-key
gpg (GnuPG) 1.4.5; Copyright (C) 2006 Free Software Foundation, Inc.
This program comes with ABSOLUTELY NO WARRANTY.
This is free software, and you are welcome to redistribute it
under certain conditions. See the file COPYING for details.

gpg: directory `/home/xsedesig/.gnupg' created
gpg: new configuration file `/home/xsedesig/.gnupg/gpg.conf' created
gpg: WARNING: options in `/home/xsedesig/.gnupg/gpg.conf' are not yet active during this run
gpg: keyring `/home/xsedesig/.gnupg/secring.gpg' created
gpg: keyring `/home/xsedesig/.gnupg/pubring.gpg' created
Please select what kind of key you want:
   (1) DSA and Elgamal (default)
   (2) DSA (sign only)
   (5) RSA (sign only)
Your selection? 5
RSA keys may be between 1024 and 4096 bits long.
What keysize do you want? (2048) 4096
Requested keysize is 4096 bits
Please specify how long the key should be valid.
         0 = key does not expire
      <n>  = key expires in n days
      <n>w = key expires in n weeks
      <n>m = key expires in n months
      <n>y = key expires in n years
Key is valid for? (0) 730
Key does not expire at all
Is this correct? (y/N) y

You need a user ID to identify your key; the software constructs the user ID
from the Real Name, Comment and Email Address in this form:
    "Heinrich Heine (Der Dichter) <heinrichh@duesseldorf.de>"

Real name: XSEDE
Email address: help@xsede.org
Comment:
You selected this USER-ID:
    "XSEDE Software <help@xsede.org>"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? O
```

The XSEDE GPG signature key was created 2014-1-29 as shown below:

```
[xsedesig@software ~]$ gpg --list-keys
/home/xsedesig/.gnupg/pubring.gpg
---------------------------------
pub   4096R/20423DBB 2014-01-31
uid                  XSEDE Software <help@xsede.org>
```

References

- GPG Best Practices