ctools - Action #1949

Feature # 1932 (Closed): Add package build and check functionality to ctools

Sign packages

03/13/2017 02:59 PM - Brau-Nogué Sylvie

Status:	Closed	**Start date:**	03/13/2017
Priority:	Normal	**Due date:**	03/23/2017
Assigned To:	Brau-Nogué Sylvie	**% Done:**	100%
Category:		**Estimated time:**	0.00 hour
Target version:			

Description

Try GPG, same signature whatever the system

TODO :

- generate GPG on a Linux machine,
- then copy to a MacOS platform
- finally sign a dmg package with this signature

- same sequence from MacOS to Linux

Related issues:

Related to ctools - Bug # 3448: Installation of ctools-1.7.2 Mac OS X binary ...	**Closed**	**11/13/2020**

History

#1 - 03/15/2017 09:12 AM - Brau-Nogué Sylvie

- Status changed from New to In Progress

- % Done changed from 0 to 20

Method

Use Case 1: generate GPG key, and rpm on the same platform	
generate GPG key	
Case 1 * product an unsigned rpm package * sign rpm package with local key	Case 2 * product a signed rpm package
Use Case 2: the same GPG key for all platforms	
generate key on the Remote Key Server	
import the GPG key	
Case 1 * product an unsigned rpm package * sign rpm package with local key (imported)	Case 2 * product a signed rpm package
Use Case 3: a single GPG Key Server	
generate a GPG key on the signature server	
on each local platform	-> product an unsigned rpm package
copy the package on the signature server	
on the signature server	-> sign the rpm packages and deploy

#2 - 03/15/2017 09:32 AM - Brau-Nogué Sylvie

- Tags set to PACKAGING

Case 1: local only

{{collapse(gpg --gen-key)}}

{{collapse(gpg --list-public-keys)

```
/home/osboxes/.gnupg/pubring.gpg
--------------------------------
pub   048R/0D76EA78 2017-03-14
uid                  turlututu (encore un test) <mytests@gmail.com>
sub   2048R/13A2B2B1 2017-03-14
```

}}

{{collapse(gpg -K)

```
/home/osboxes/.gnupg/secring.gpg
--------------------------------
sec   2048R/0D76EA78 2017-03-14
uid                  turlututu (encore un test) <mytests@gmail.com>
ssb   2048R/13A2B2B1 2017-03-14
-----> The GPG key ID is %{color:tomato}*0D76EA78*%
```

```
echo "%_gpg_name 0D76EA78 " >> ~/.rpmmacros
```

}}

{{collapse(Update ~/.rpmmacros)
more ~/.rpmmacros

```
%packager       Sylvie Brau-Nogue <sylvie.brau-nogue@irap.omp.eu>
%vendor         irap.omp.eu repo http://cta-gitlab.irap.omp.eu/
%_topdir %(echo $HOME)/rpmbuild
%_tmppath %(echo $HOME)/rpmbuild/tmp
%_signature gpg
%_gpg_path %(echo $HOME)/.gnupg
%_gpg_name 0D76EA78
%_gpgbin /usr/bin/gpg
# %_smp_mflags  -j3
# %__arch_install_post   /usr/lib/rpm/check-rpaths   /usr/lib/rpm/check-buildroot
```

}}

{{collapse(gpg --export -a "turlututu (encore un test)" > RPM-GPG-KEY-example-2-signing-key)}}

{{collapse(Import a GPG key for RPM)

```
sudo rpm --import RPM-GPG-KEY-example-2-signing-key
```

}}

{{collapse(rpm -qa gpg-pubkey*)

```
gpg-pubkey-9c547790-58c80682
gpg-pubkey-43e21a06-58c7e830
gpg-pubkey-352c64e5-52ae6884
gpg-pubkey-b3d28d79-58c7fb78
gpg-pubkey-e88bdf30-58c7e2ef
gpg-pubkey-f4a80eb5-53a7ff4b
```

gpg-pubkey-eefefde9-58999f26
gpg-pubkey-0d76ea78-58c85a6a

}}

{{collapse(rpm -qi gpg-pubkey-0d76ea78-58c85a6a)

```
Name        : gpg-pubkey
Version     : 0d76ea78
Release     : 58c85a6a
Architecture: (none)
Install Date: mar. 14 mars 2017 21:13:23 GMT
Group       : Public Keys
Size        : 0
License     : pubkey
Signature   : (none)
Source RPM  : (none)
Build Date  : mar. 14 mars 2017 21:02:34 GMT
Build Host  : localhost
Relocations : (not relocatable)
Packager    : turlututu (encore un test) <sbn.pub@gmail.com>
Summary     : gpg(turlututu (encore un test) <sbn.pub@gmail.com>)
Description :
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: rpm-4.11.3 (NSS-3)

mQENBFjIWmoBCADiX45BopLcOPx/Lz50bruRhGJrEuNRDJupUSTATKDulTjHb8pa
CSEFhuIZPKsBXERz5+gHnq3pjOBu6Ztds4l0iLxl23zOoDlSmxz+dT6R7nZ7+XWw
zY2lJ5emudgfq9l0XXR2uYDToZPRwfrC1C/yr8KS72hXDsRPVbkUMYvnld8OEH9i
8dRSOVPo+hzg6AZoepRlmde4sospzl/aJXB2BduYmIqnlL3GpeOQvrBOhqV14J1B
34l30CoM6pfviqn1+0rm8lklIhKZ5LkyMdnC0pph4LrfbR0xDewYVE1iDTpr7OPgQ
5DbSr9l5Lhm/3bTkjaUruPx67mUWf9Fb2rm/ABEBAAG0LnR1cmx1dHV0dSAoZW5j
b3JlIHVuIHRlc3QpIDxzYm4ucHViQGdtYWlsLmNvbT6JATkEEwECACMFAIjIWmoC
GwMHCwkIBwMCAQYVCAIJCgsEFgIDAQIeAQIXgAAKCRDuOc2fDXbqePwtCADhZbwM
qko1uX0r/CQNZtFrzfMkL2dVG1DG7JdMyKi9dRj7QxPNZ82ay+61uGuOX53qWvnG
BHLvJ2stklQtYinOJrc9Q+YjXNCmJDFv2fmFEyiTqjZP9MaaaJbrwcn+B9c2d7la
UcxhYGE8XhSJqrsL8lnrID3qzQiW30NcxCNb+rY5y09e61seGZZB5n4p8o3C1XHv
iz2Galr75QkPP3Eje0ZJY1+VsCCyP48KmRYkZkrG5gO/2PkNnrEj1EMDaz6FQaF/
wJBs+WTy1s3uqV1dDPyLTASPMZittXxqnXwMXkiuUSHw3aqr7GkHu11OZiGyz5TJ
QkYIIWCTv7JoXNnquQENBFjIWmoBCADtiemLP6YUHx6pcV4zAygMbeF3hNk2JSNU
Q97yg4BPYjb1apRL+8rAUfmv1kbXe0ccqsmFN0t8QkcepM2P2y2o2oofdpV3W5ma
yHucBkDbagYJ+XyRKT3fCs19VxVn7ijyfTeY6moWVZUSfGhQvZSze8VlFDW0Srr5
m+w5QSMY31YtFN1MhxtTmI5jkTMLEYv/ZS8Tf4kDFVHGNER5gZIm3yZLmZADAVTl
MgwZXsVRTyzVG0KNeOUAaj2/9lKrtBpugy68sfieTSXWcihs8+cPdABO7g2tVfWs
Bi+HonLQlHuxp8SDIF0o2hOj62Y4vGH8DSIvVqMGOUfDFFfnL5w3ABEBAAGJAR8E
GAECAAkFAIjIWmoCGwwACgkQ7jnNnw126ngjvwgAm9X7VVeepo1W5kIm/9047uzL
c6DP+UazJb//arT00b7rVK78K/GS+n2i1GwIZYf6CzVJOZPcor5nIQ/OL5/WNpPc
8MwBQzpu9aTHhjn1OFJgFX+FwdVUFjtcO593/+S467lYQWjwhlfOnaL0yE3maqND
fix08wcfrg2U9TvLFKPvuKlJrrgm2YRFh8nss4A6+CZE6JflY8xQAr37etnuyVN4
YMdIlenDnCkmHUw0cKdaZmkfKDI7WECmkdsRzhB4V6q7zs9QxmzHepGVMwU7rjBF
dybiIyB51+tzhjuJYMM/dEu09IA4BzQOda++Oaf1pr5gbBnsHGzverKVQyt93g==
=8cv8
-----END PGP PUBLIC KEY BLOCK-----
```

}}

Sign a rpm package

{{collapse(rpm --addsign -v ctools-1.2.0.dev1-1.el7.centos.x86_64.rpm)

```
Entrez la phrase de passe :
Phrase de passe bonne.
ctools-1.2.0.dev1-1.el7.centos.x86_64.rpm:
```

rpm -qip ctools-1.2.0.dev1-1.el7.centos.x86_64.rpm

```
attention : ctools-1.2.0.dev1-1.el7.centos.x86_64.rpm: Entête V4 RSA/SHA1 Signature, clé ID 0d76ea78: NOKEY
Name        : ctools
```

```
Version     : 1.2.0.dev1
Release     : 1.el7.centos
Architecture: x86_64
Install Date: (not installed)
Group       : Development/Libraries
Size        : 56567703
License     : GPLv3
Signature   : RSA/SHA1, mar. 14 mars 2017 21:09:31 GMT, Key ID ee39cd9f0d76ea78
Source RPM  : ctools-1.2.0.dev1-1.el7.centos.src.rpm
Build Date  : mar. 14 mars 2017 13:53:02 GMT
Build Host  : osboxes
Relocations : /usr/local/gamma
Packager    : Sylvie Brau-Nogue <sylvie.brau-nogue@irap.omp.eu>
Vendor      : irap.omp.eu repo http://cta-gitlab.irap.omp.eu/
URL         : http://cta.irap.omp.eu/ctools
Summary     : Versatile toolbox for scientific analysis of astronomical gamma-ray data
Description :
Cherenkov Telescope Array Science Analysis Software


}}
```

Integrate signature in pkgbuild-centos.sh

PROBLEM : the script stops by waiting for the pass phrase
or "How to provide password to a command that prompts for one in bash?"

use expect

sudo yum install expect

Declare the passphrase in an environment variable when logging in

1. file **.bashrc**

   ```
   GPG_PASSPHRASE="xxxxxx this my pass phase xxxxxxx"
   export GPG_PASSPHRASE
   ```

2. Another possibility to create a **specific file** in .gnupg directory

   at login script, extract pass phrase from this file

<<<<< see this page, or this article >>>>>

then signature, 2 options

case 1 : in Makefile

```
rpm-sign:
   (\
     echo set timeout -1;\
     echo spawn rpmsign --addsign target/rpmbuild/RPMS/*/*.rpm;\
     echo expect -exact \"Enter pass phrase:\";\
     echo send -- \"$(GPG_PASSPHRASE)\\r\";\
     echo expect eof;\
   ) | expect
```

case 2 : in pkgbuild-centos.sh

```
# ================================================== #
# Sign package with pass phrase set during login
 (\
   echo set timeout -1;\
   echo spawn rpmsign --addsign $PKGDIR/*/*.rpm;\
   echo expect -re \"pass\";\
```

```
  echo send -- \"$GPG_PASSPHRASE\\r\";\
  echo expect eof;\
) | expect
```

#3 - 03/16/2017 11:27 AM - Brau-Nogué Sylvie

- % Done changed from 20 to 100

Finally, the best choice is Use Case 3: a single GPG Key Server

1. generate a GPG key on the signature server
2. on each local platform -> product an unsigned rpm package
3. transfert the package on the signature server
4. on the signature server -> sign the rpm packages and deploy

Many reasons, the most important of which is to guarantee the signature of the package with the latest GPG signature

#4 - 03/23/2017 12:19 PM - Knödlseder Jürgen

On Mac OS X 10.11 I created a "S/MIME" certificat with the keychain tool. I was then able to sign the package on my Mac as follows:

```
$ productsign --sign 'ctools-2' ctools-1.2.0.pkg /Users/jurgen/ctools-1.2.0-signed.pkg
productsign: signing product with identity "ctools-2" from keychain /Users/jurgen/Library/Keychains/login.keychain
productsign: Wrote signed product archive to /Users/jurgen/ctools-1.2.0-signed.pkg
```

Note that I did not manage to sign the package with a "Code Signing" Certificat.

I tried the same on the Mac OS X 10.7 VM which is the machine where the OS X package is built. However on that platform the signing did not work:

```
$ productsign --sign 'ctools' ctools-1.3.0.dev1.pkg ctools-1.3.0.dev1-signed.pkg
productsign: signing product with identity "ctools" from keychain /Users/jenkins/Library/Keychains/login.keychain
Error signing data.
productsign: error: Failed to sign the product.
```

Unfortunately there is no more information available explaining what happened.

#5 - 03/23/2017 12:34 PM - Knödlseder Jürgen

No access to the ctools private key was granted. This can be changed in the Keychain Access application by double clicking on the ctools private key. Once this is done it worked:

```
$ productsign --sign 'ctools' ctools-1.3.0.dev1.pkg ctools-1.3.0.dev1-signed.pkg
productsign: signing product with identity "ctools" from keychain /Users/jenkins/Library/Keychains/login.keychain
productsign: Wrote signed product archive to ctools-1.3.0.dev1-signed.pkg
```

#6 - 03/23/2017 12:41 PM - Knödlseder Jürgen

I added the signature to the Mac OS X product build step:

```
# Build product
productbuild --distribution $DISTFILE \
        --version $VERSION \
        --resources $SRCDIR/$CTOOLS \
        --package-path $PKGDIR \
        --sign 'ctools' \
        $PRODDIR/$CTOOLS.pkg
```

This gave

```
...
pkgbuild: Inferring bundle components from contents of /usr/local/gamma
pkgbuild: Writing new component property list to /Users/jenkins/jenkins/workspace/ctools-cr-osx/pkg_build/pkg/ctools-1.3.0.dev1-components.plist
pkgbuild: Reading components from /Users/jenkins/jenkins/workspace/ctools-cr-osx/pkg_build/pkg/ctools-1.3.0.dev1-components.plist
pkgbuild: Wrote package to /Users/jenkins/jenkins/workspace/ctools-cr-osx/pkg_build/pkg/ctools-1.3.0.dev1.pkg
productbuild: Wrote synthesized distribution to /Users/jenkins/jenkins/workspace/ctools-cr-osx/pkg_build/prod/ctools-1.3.0.dev1.dist
productbuild: Signing product with identity "ctools" from keychain /Users/jenkins/Library/Keychains/login.keychain
productbuild: Wrote product to /Users/jenkins/jenkins/workspace/ctools-cr-osx/pkg_build/prod/ctools-1.3.0.dev1.pkg
.....................................................................
created: /Users/jenkins/jenkins/workspace/ctools-cr-osx/pkg_build/ctools-1.3.0.dev1-macosx10.7.dmg
```

Looks like it worked.

#7 - 03/23/2017 02:09 PM - Knödlseder Jürgen

For some reason, implementing the signature in the continuous release did not work:

```
pkgbuild: Inferring bundle components from contents of /usr/local/gamma
pkgbuild: Writing new component property list to /Users/jenkins/jenkins/workspace/ctools-cr-osx/pkg_build/pkg/ctools-1.3.0.dev1-components.plist
pkgbuild: Reading components from /Users/jenkins/jenkins/workspace/ctools-cr-osx/pkg_build/pkg/ctools-1.3.0.dev1-components.plist
pkgbuild: Wrote package to /Users/jenkins/jenkins/workspace/ctools-cr-osx/pkg_build/pkg/ctools-1.3.0.dev1.pkg
productbuild: Wrote synthesized distribution to /Users/jenkins/jenkins/workspace/ctools-cr-osx/pkg_build/prod/ctools-1.3.0.dev1.dist
Error signing data.
productbuild: error: Could not sign product at "/Users/jenkins/jenkins/workspace/ctools-cr-osx/pkg_build/prod/ctools-1.3.0.dev1.pkg".
productbuild: Signing product with identity "ctools" from keychain /Users/jenkins/Library/Keychains/login.keychain
```

#8 - 03/23/2017 02:44 PM - Knödlseder Jürgen

The reason was that Jenkins does not automatically unlock the local keychain. Adding

```
security unlock-keychain -p password login.keychain
```

solved the issue. However, since we don't want to type the password visibly, another solution was moving the ctools certificate to the System.keychain.

#9 - 03/23/2017 03:00 PM - Knödlseder Jürgen

Seems to work now:

```
productbuild: Wrote synthesized distribution to /Users/jenkins/jenkins/workspace/ctools-cr-osx/pkg_build/prod/ctools-1.3.0.dev1.dist
productbuild: Signing product with identity "ctools" from keychain /Library/Keychains/System.keychain
productbuild: Wrote product to /Users/jenkins/jenkins/workspace/ctools-cr-osx/pkg_build/prod/ctools-1.3.0.dev1.pkg
created: /Users/jenkins/jenkins/workspace/ctools-cr-osx/pkg_build/ctools-1.3.0.dev1-macosx10.7.dmg
```

#10 - 06/07/2017 05:49 PM - Knödlseder Jürgen

- Target version changed from 1.3.0 to 1.4.0

#11 - 08/01/2017 09:54 AM - Knödlseder Jürgen

- Target version changed from 1.4.0 to 1.5.0

#12 - 01/23/2018 12:13 PM - Knödlseder Jürgen

- Target version deleted (1.5.0)

#13 - 04/03/2018 11:57 AM - Brau-Nogué Sylvie

- Status changed from In Progress to Closed

#14 - 11/16/2020 02:19 PM - Knödlseder Jürgen

- Related to Bug #3448: Installation of ctools-1.7.2 Mac OS X binary disk image failed on mac OS Catalina added