Tails - Bug #12733
Seahorse fails to import private PGP keys: pinentry-gtk-2 passphrase prompt not displayed
06/19/2017 07:50 AM - goupille

Status: Resolved
Priority: Elevated
Assignee: goupille
Category: Security
Target version: Tails_3.2
Feature Branch: bugfix/12733-seahorse-vs-pinentry-gtk2
Type of work: Code
Blueprint: Seahorse Preferable

Description:
to reproduce this:
create a PGP key with seahorse (4096-bits)
export the private key in .asc format and delete the original key
then try to import it from seahorse.
the importation fails with this error:
keyserver option ‘ce-cert-filv’ is unknown

Related issues:
- Related to Tails - Bug #10941: seahorse-tool --import does not import keys co... Resolved 01/14/2016
- Related to Tails - Bug #11099: Decide which pinentry we want to ship Resolved 02/09/2016
- Related to Tails - Feature #9555: Include a pinentry GUI that's well integrat... Rejected 06/10/2015
- Blocks Tails - Feature #13234: Core work 2017Q3: Foundations Team Resolved 06/29/2017

Associated revisions
Revision ea71d015 - 08/12/2017 06:01 PM - intrigeri
Ensure pinentry-gtk2 run by Seahorse has the correct $DISPLAY set (refs: #12733).
As discussed in more details on https://bugs.debian.org/869416, there's a bug
somewhere in the Seahorse → gnupg-agent → pinentry-gtk2 communication, that
leads to pinentry-gtk2 being invoked with the $DISPLAY environment variable
being unset. Strangely, this does not happen for gpg → gnupg-agent →
pinentry-gtk2. Now that upstream is aware of the problem, let's apply
a temporary workaround to Tails until the root cause is fixed.

Revision 975245bb - 08/15/2017 11:29 AM - anonym
Merge remote-tracking branch 'origin/bugfix/12733-seahorse-vs-pinentry-gtk2' into stable
Fix-committed: #12733

History
#1 - 06/19/2017 03:48 PM - tailserr0r
goupille wrote:
to reproduce this:

create a PGP key with seahorse (4096-bits)
export the private key in .asc format and delete the original key
then try to import it from seahorse.

the importation fails with this error:

keyserver option 'ce-cert-filv' is unknown

I have a similar issue, all the keys in "private-keys-v1.d" from older tails will not import. When trying to drag and drop into key manager I get:

Reason: Unrecognized or unsupported data.

Via cmd line with gpg2 --import *.key I get:

gpg: no valid OpenPGP data found.
gpg: Total number processed: 0

Most keys in that dir are around 2570 bytes, so not empty.

When I upgraded to 3.0 I had a expired tails developers key and when downloading the updated signing key from https://tails.boum.org/tails-signing.key, I could not import it I would get a "Keys were found but not imported" when double clicking, and a odd error msg when dragging and dropping into key manager that said "failed to import (key name) imported".

so it would say it both failed and imported it, though it would never import. At the time I did not try via cmd line so unsure the specific error there.

After doing this several times it did finally manage to import, and my entire key ring with dozens of keys went missing. The tails developers key stayed though. Upon reboot, my keys were back and the signing key stuck. This was a week ago.

Yesterday I noticed some keys were missing. I had backed up my gnupg folder to a freshly installed tails 3.0 usb and booted into it to find some of the missing keys were there, but not all. Interestingly, some keys that I had imported the same day as others were missing. It appears that 3.0 is being very selective about which keys to retain, maybe related to this particular bug? Fortunately none of these keys were critical or I could have lost years of work.

I find it strange that one freshly upgraded tails 3.0 did not display keys that another freshly installed tails 3.0 showed, despite both of them using the same gnupg folder contents. I was able to import my pubring.pgp and get some of the missing keys back, others I had to export from the other backup to .asc and then import them to my current install.

Those 4096 keys made in tails 2.13 as a .asc file are able to be imported fine.

Hopefully this information helps.
#2 - 06/19/2017 04:42 PM - emmapeel
- Related to Bug #10941: seahorse-tool --import does not import keys completely added

#3 - 06/19/2017 04:42 PM - emmapeel
Sounds a bit like #10941. Can you try importing them with gpg --import [keyfile]?

#4 - 06/27/2017 01:15 PM - Anonymous
I just tried this in Tails 3.0:
create a PGP key with seahorse (4096-bits)
export the private key in .asc format and delete the original key
close then reopen seahorse
then try to import it from seahorse.

The importation pretends to fail, saying "Key not imported" then I click again on "Import" and then I get: "No valid OpenPGP data found". When I close seahorse and then reopen it, the key has actually been imported partly: only the public key shows up.

When I do the import manually, I'm asked for my passphrase and then the private key also shows up in Seahorse (after closing and reopening it).

The asc is a correct private key file.

#5 - 06/28/2017 04:52 PM - intrigeri
- Assignee changed from anonym to intrigeri
- Target version set to Tails_3.1

During the help desk / foundations team meeting today, we deemed this ticket as high-priority (from a user-centric PoV). So adding to my plate at least to investigate a bit closer.

#6 - 06/29/2017 10:22 AM - intrigeri
- Blocks Feature #13234: Core work 2017Q3: Foundations Team added

#7 - 06/29/2017 08:43 PM - intrigeri
- Subject changed from Seahorse fails to import private PGP keys to Seahorse fails to import private PGP keys: pinentry-gtk-2 passphrase prompt not displayed

[@dkg: of course you don't have to look at this bug report before I report it to Debian, but if you want & have some time, your insight would be welcome.]
@goupille: a workaround is to add this line:

```
pinentry-program /usr/bin/pinentry-gnome3
```

… to ~/.gpg/gpg-agent.conf. IIRC (#11099) the downside is that this pinentry grabs the mouse and keyboard, so one cannot go fetch a passphrase in KeePassX after having been asked for it. No idea if KeePassX' global keyboard shortcut works in there but I guess it doesn't.

So, I've tried about the same, using the default key creation settings, in a clean and up-to-date sid VM, after exporting a key both in armored and binary format from Seahorse, and doing View → Show Any (the default being Show Personal): both importing she binary (.pgp) and armored (.asc)
keys works fine. But in each case, only the pubkey is imported, which is not surprising as the key exported by Seahorse is the pubkey only (that's kinda good news given the amount of times people sent me their private key due to Seahorse in Jessie exporting that one by default). So far, that's only intended behavior. Then I tried the same in Tails 3.0 and observed exactly the same behavior.

Still, I wanted to test what the ticket title says. At this point, I don't know how exactly goupille and u tried, since "export the private key in .asc format and delete the original key" doesn't tell me how the key was exported.

So I've exported the armored private key using gpg on the command line, and when trying to import it using Seahorse I'm told Import failed: key 0x...: public key "uid <email>" imported. If I click "Import" again I'm told Import failed: no valid OpenPGP data found, and then clicking "Cancel" doesn't work. The newly imported key doesn't show up in Seahorse, but gpg tells me that the public part has been imported, while the private part hasn't. Interesting. This matches what u reported, good! The Journal says:

gpg-agent[10683]: command 'IMPORT_KEY' failed: Inappropriate ioctl for device <Pinentry>.

So again, gpg-agent has issues talking to pinentry-gtk-2 when used by seahorse, while it works fine when using gpg in GNOME Terminal.

Then I've used update-alternatives to configure pinentry-gnome3 instead of pinentry-gtk-2 for the pinentry and pinentry-x11 alternatives, because, well, who knows. I've retried, and this time everything worked fine: both the public and private keys were correctly imported. At this point I'm very much tempted to blame pinentry-gtk-2, but I'm biased (I was opposed to the collective decision that said we should use this one instead of pinentry-gnome3 in the first place). I've checked (/proc/PID/environ) that both gpg-agent and seahorse run with the correct $DISPLAY set in their environment, and using gpg on the command line correctly starts pinentry-gtk-2. The difference I see in gpg-agent's debug log is that when using pinentry-gnome3, I see a number of OPTION commands sent to gpg-agent, e.g. OPTION display=:1, while I see no such thing when using pinentry-gtk-2. I'm not sure who's responsible for sending these options.

I've already spent more than 2 hours on this, and I've almost reached the limits of my comfort zone technically, so I'll reproduce on sid and will report to Debian to get debugging hints from better skilled people.
- Related to Bug #11099: Decide which pinentry we want to ship added

- Related to Feature #9555: Include a pinentry GUI that's well integrated within GNOME added

- Status changed from Confirmed to In Progress

- Target version changed from Tails_3.1 to Tails_3.2
- % Done changed from 0 to 10

Reported as https://bugs.debian.org/869416. I'll debug this further if/once I'm given instructions.

If no realistic solution to this problem arises soon, I'll check how pinentry-gnome3 works with KeePassX these days (in particular wrt. it global keyboard shortcut), with the idea in mind of perhaps revisiting our decision to ship pinentry-gtk2 with the new info we now have (i.e. some basic functionality is broken when using that pinentry implementation, which might weight more than "pinentry-gnome3 is harder to use with KeePassX" at the end of the day).

segfault: IIRC you were the strongest proponent of pinentry-gtk2, so you might be interested in having a look at this ticket :)

- Assignee changed from intrigeri to anonym
- % Done changed from 10 to 50
- QA Check set to Ready for QA
- Feature Branch set to bugfix/12733-seahorse-vs-pinentry-gtk2
- Type of work changed from Research to Code

Fixes a regression introduced in 3.0. (Meta: trying to help anonym prioritize his pile of reviews :)

- Status changed from In Progress to 11
- Assignee deleted (anonym)
- % Done changed from 50 to 100
- QA Check changed from Ready for QA to Pass

- Status changed from 11 to Resolved