

AqBanking - Bug #287

valid gpg keyring for verification missing?

26.08.2022 18:21 - ilippert

Status:	Feedback	Beginn:	26.08.2022
Priorität:	Normal	Abgabedatum:	
Kategorie:	Libchipcard	Anwendung:	andere
Betriebssystem:	Linux	Version der Anwendung:	
AqBanking-Version:	none		
Beschreibung Hello, downstream, in the Fedora project, we are looking for a keyring to verify the package. Would you be able to clarify whether the source package contains any? https://bugzilla.redhat.com/show_bug.cgi?id=2035958 Cheers Ingmar			

Historie

#1 - 27.08.2022 00:17 - martin

- Status wurde von New zu Feedback geändert

Hi,

I'm sorry, but what do you mean by that? We don't provide packages, what keyring are you referring to?

Regards
Martin

#2 - 27.08.2022 01:01 - ilippert

Hi Martin,
äh, sorry,
So, the packages come with pgp asc files

We, at Fedora, try to package Libchipcard :)

Now, we have found a gpg key that should supposedly work for
<https://www.aquamaniac.de/rdm/attachments/381/libchipcard-5.1.6.tar.gz.asc>

that is: gpgkey-42400AF5EB2A17F0A69BB551E9899D784A977416.gpg

but that key is found to not be working by the packaging team.

So, the question better is: which key to use to verify the signature?
where is a key provided to verify, they ask.
Cheers,
Ingmar

#3 - 04.10.2022 20:31 - ilippert

Also die Frage bezieht sich auf
<https://www.aquamaniac.de/rdm/attachments/download/381/libchipcard-5.1.6.tar.gz.asc>
Das scheint eine Signaturdatei zu sein.

Frage: mit welchem öffentlichen Schlüssel lässt sich die Signatur verifizieren?

#4 - 06.10.2022 11:51 - ipwizard

Das wäre <https://keyserver.ubuntu.com/pks/lookup?search=0x4A977416&fingerprint=on&op=index> Dem würde ich aber nicht über den Weg trauen.
Schon einige Jahre alt und nur von sich selbst signiert.

#5 - 06.10.2022 12:04 - ilippert

Danke, dann die Frage: wäre es möglich, einen vertrauenswürdigeren Schlüssel zum Signieren heranzuziehen und die Signaturen dann mit zu veröffentlichen? Bzw, ließe der Schlüssel sich vertrauenswürdiger gestalten? Oder soll es so bleiben wie es ist?

#6 - 06.10.2022 18:19 - ilippert

Fascinatingly, the Fedora software volunteers are not able to verify the signature with that key - https://bugzilla.redhat.com/show_bug.cgi?id=2035958#c20

Martin, any alternative key you could point to?

#7 - 06.10.2022 21:09 - martin

This is the key I use to sign source packages for the AqBanking family, currently no alternative key.
I can't reproduce the key problem, here I can verify the signature of the package:

```
#> gpg --verify libchipcard-5.99.1beta.tar.gz.asc
gpg: assuming signed data in 'libchipcard-5.99.1beta.tar.gz'
gpg: Signature made Sat Sep 25 14:08:47 2021 CEST
gpg:                using RSA key 42400AF5EB2A17F0A69BB551E9899D784A977416
gpg: Good signature from "AqBanking Package Key <packages@aqbanking.de>" [ultimate]
```

#8 - 06.10.2022 22:15 - ilippert

Unfortunately, I get

```
gpg --verify /tmp/libchipcard-5.1.6.tar.gz.asc
gpg: assuming signed data in '/tmp/libchipcard-5.1.6.tar.gz'
gpg: Signature made Fri 17 Sep 2021 17:46:42 CEST
gpg:                using RSA key 42400AF5EB2A17F0A69BB551E9899D784A977416
gpg: BAD signature from "AqBanking Package Key <packages@aqbanking.de>" [unknown]
```

and also for

```
gpg --verify /tmp/libchipcard-5.99.1beta.tar.gz.asc
gpg: assuming signed data in '/tmp/libchipcard-5.99.1beta.tar.gz'
gpg: Signature made Sat 25 Sep 2021 14:08:47 CEST
gpg:                using RSA key 42400AF5EB2A17F0A69BB551E9899D784A977416
gpg: BAD signature from "AqBanking Package Key <packages@aqbanking.de>" [unknown]
```

#9 - 06.10.2022 22:18 - ilippert

And I even trust the key "fully"

```
gpg --edit-key 42400AF5EB2A17F0A69BB551E9899D784A977416
  1
gpg (GnuPG) 2.3.7; Copyright (C) 2021 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

pub  rsa2048/E9899D784A977416
     created: 2017-08-08  expires: never           usage: SC
     trust: full          validity: unknown
sub  rsa2048/87400BDBD5B77CD4
     created: 2017-08-08  expires: never           usage: E
[ unknown] (1). AqBanking Package Key <packages@aqbanking.de>
```

#10 - 07.10.2022 20:54 - martin

Hmm, does your checksum match that on the download page? I just downloaded the files and md5sum matches the data in the download page column:

```
#> md5sum libchipcard-5.99.1beta.tar.gz*
bf97547fc4ae2f1fb8460f50ba386f7f  libchipcard-5.99.1beta.tar.gz
db76ff8563d9fea6b1c0591a3c36577c  libchipcard-5.99.1beta.tar.gz.asc
```

#11 - 11.10.2022 09:42 - ilippert

Hmm, I did not pursue this personally (too busy as everybody), but some other Fedora community person managed to verify the key.

So, this issue can be closed.

Meanwhile for your information, the packaging at Fedora succeeded. Now the package lives there at <https://src.fedoraproject.org/rpms/libchipcard>

You are welcome to join there as co-maintainer (I am saying this without any expectations, of course)!

Thanks for your support!