openSUSE admin - tickets #89029

OpenSuse GPG keys in DNS

2021-02-23 18:36 - msuchy@redhat.com

Status:	Closed	**Start date:**	2021-02-23
Priority:	Normal	**Due date:**	
Assignee:	opensuse-admin-obs	**% Done:**	100%
Category:	Core services and infra	**Estimated time:**	0.00 hour
Target version:			

Description

Hi.
I am working on enhancing of verifying GPG checks of RPM packages using GPG keys stored in DNS entries. I want to ask you to store OpenSuse's GPG keys its DNS zone.

This is likely something new to you. So I provide you with some reading and the background:

http://miroslav.suchy.cz/blog/archives/2021/02/11/verify_package_gpg_signature_using_dnssec/index.html

http://miroslav.suchy.cz/blog/archives/2021/02/13/how_to_generate_openpgp_record_for_dns_type61/index.html

http://miroslav.suchy.cz/blog/archives/2021/02/18/different_opengpg_dns_entries_for_the_same_email/index.html

The last two are most relevant for what you need.

OpenSuse GPG keys are here:

https://build.opensuse.org/projects/openSUSE:Factory/public_key

Here is a detailed howto to what needs to be done:

1. Save the file above as RPM-GPG-KEY-openSUSE

2. $ gpg2 RPM-GPG-KEY-openSUSE
   pub rsa2048 2008-11-07 [SC] [platnost skončí: 2024-05-02]
   22C07BA534178CD02EFE22AAB88B2FD43DBDC284
   uid openSUSE Project Signing Key opensuse@opensuse.org

Note the used email.

1. Import the GPG key to your local keyring:

$ gpg2 --import RPM-GPG-KEY-openSUSE

1. run: $ gpg2 --export-options export-dane --export 'opensuse@opensuse.org'

This will generate a DNS entry. You have to put it in _openpgpkey.opensuse.org. DNS zone.

It should be:

```
$ORIGIN _openpgpkey.opensuse.org.
; 22C07BA534178CD02EFE22AAB88B2FD43DBDC284
; openSUSE Project Signing Key <opensuse@opensuse.org>
791f5d38084c356de75bcb606c65cd04be8b1928b6e364861c01ecce TYPE61 \# 645 (
99010d0449144c3f010800d62f2e5de48a4979d1d04125e40b554afe80199491
1e055a526633029fc2e21da23d5aadc6dd5a7ac2fb0fd5bde4b2c246cd514d72
d757b79b63bce2f1beb11f449b867ea1d32882c1caa2f391ec966b06c535f490
f77ffc3ae9df4935c2d52c77860b0d5d0b8eacd54aac301052a4fadb4fe38fde
31348834f5b2d2c6c8cde84793bf288e9ad13d1f5274de8f6d63a99e34bfe071
087106fc2ea36d399e9d09a236013f4a4e7cdf25f619c838b900d32bb86578a0
a0a39599fe224e35f83489885a5753f946964ced7c356702aee8ed807b9ecadc
182c1355e4dd282483f6558b8b65f483558b8f965bfb73a3b650439726c75b41
```

```
a56ecd4d472e8703ca2a670011010001b4346f70656e535553452050726f6a65
6374205369676e696e67204b6579203c6f70656e73757365406f70656e737573
652e6f72673e89013c041301020026021b03060b090807030204150208030416
020301021e0102178005025367 4dd405091d1f0495000a0910b88b2fd43dbdc2
84642b07ff6d78267736df2f1c4d120b936660c004d52a5c8e4cf1e8ce2be02e
f40154cc11087ff01be09b090a3ffa88096a36bc2d613174602e0fd39d3b450e
aee45be987b025e67f938b876a8e5822a2e79562b657fa6e61fb9fe877e1285a
122f2000e6d2a59485f01ccf1a5eafd1098468628cdced6851b6c1dd9f22eb0d
b509383b75b539bc647c6218bdacdb6b86aacf4beab6c9fb6335bb0e0da81a39
46fce4449f406c7f2eaa0c78f0feecca86a405e328c66ab040cfd136f14f04a4
e142a7178cc50981cf2cadf2fe1487e52109c303d8d7597a246742d547bc6736
a3edffff6b152cfe14c2d1465a104f9ae6fe206ea39c8a029a16cf4b737063f1
bfe5135d18
)
```

You can verify the work by running:

$ dig -t TYPE61 791f5d38084c356de75bcb606c65cd04be8b1928b6e364861c01ecce._openpgpkey.opensuse.org

or

$ resolvectl openpgp 'rpmfusion-buildsys@lists.rpmfusion.org`

Note, that having a domain secured by DNSSEC would be a nice thing, but this step is useful even without DNSSEC.

Miroslav Suchy, RHCA
Red Hat, Associate Manager, Community Packaging Tools, #brno, #fedora-buildsys

History

#1 - 2021-03-11 23:00 - lrupp

- Category set to Core services and infra

- Status changed from New to Workable

- Assignee set to opensuse-admin-obs

Hi Miroslav

Nice idea - 100% supported!
Let's clarify this with our DNS and Release-Gurus (which might take some time)....

Regards,
Lars

#2 - 2021-04-27 20:16 - lrupp

- Private changed from Yes to No

#3 - 2021-05-20 12:39 - lrupp

- Status changed from Workable to Feedback

One question came up here during some discussions: why not using the OPENPGPKEY resource record for this?

With kind regards,
Lars

#4 - 2021-05-21 20:24 - msuchy@redhat.com

Dne 20. 05. 21 v 14:39 redmine@opensuse.org napsal(a):

> One question came up here during some discussions: why not using the OPENPGPKEY resource record for this?

TYPE61 == OPENPGPKEY

See https://en.wikipedia.org/wiki/List_of_DNS_record_types

Miroslav

#5 - 2021-06-02 14:27 - lrupp

- % Done changed from 0 to 30

Good news: I added the following keys now to the opensuse.org domain:

- opensuse@opensuse.org (791f5d38084c356de75bcb606c65cd04be8b1928b6e364861c01ecce._openpgpkey.opensuse.org)
- buildservice@opensuse.org (3a0cfb13d70c7f6a9a5d64b4eeaf7098f0d916827efed5d96abbdc43._openpgpkey.opensuse.org - including sub-key)
- build-container@opensuse.org (f86263d23149776835fd295f9968674a1f4c5f10be7da4d5dc3ade03._openpgpkey.opensuse.org)

In addition, we are currently testing DNSSec with the opensuse.de domain. Once the key exchange (on the Registrar side) has been done and tested successfully, we can enable DNSSec as well.

Can you please check, if I did not miss something or did something wrong here?

Thanks for your support!

Regards,
Lars

#6 - 2021-06-03 10:44 - msuchy@redhat.com

Dne 02. 06. 21 v 16:27 redmine@opensuse.org napsal(a):

> Good news: I added the following keys now to the opensuse.org domain:
> *opensuse@opensuse.org (791f5d38084c356de75bcb606c65cd04be8b1928b6e364861c01ecce._openpgpkey.opensuse.org)
> *buildservice@opensuse.org (3a0cfb13d70c7f6a9a5d64b4eeaf7098f0d916827efed5d96abbdc43._openpgpkey.opensuse.org - including sub-key)
> *build-container@opensuse.org (f86263d23149776835fd295f9968674a1f4c5f10be7da4d5dc3ade03._openpgpkey.opensuse.org)
>
> In addition, we are currently testing DNSSec with the opensuse.de domain. Once the key exchange (on the Registrar side) has been done and tested successfully, we can enable DNSSec as well.
>
> Can you please check, if I did not miss something or did something wrong here?

I can completely check only the opensuse@opensuse.org as I have this key. Yes. It is done correctly and I can verify it.

The other keys seems to be implemented correctly as well, but I did not compared the actuall value, because I do not have the key.

Thank you for the work.

Regards

Miroslav Suchy

#7 - 2021-08-09 20:01 - lrupp

- Status changed from Feedback to Closed

- % Done changed from 30 to 100

ok, closing the ticket here, as the initial request is done.

Thanks for your support!