PgpKeySigning

We will have a PGP Key Signing at the ApacheConEU 2019. It will happen Thursday, 13:00-14:00 in the Hackathon room.

Remember: you can always sign keys individually throughout the conference. Feel free to ask around: if you meet other people from your project in person, they often will be willing to sign keys. Some people print up simple business cards or small slips of paper with their name, email, and PGP key fingerprints to pass out.

Preparation

- Make sure you have send your public key to a keyserver (keyserver.ubuntu.com)
- Register to the keysigning using https://docs.google.com/forms/d/1V08IpxdYQl-RwPsh3tvmDvTDv02DQoJ7-3p8Qutm5LI/ with our your long key-id as soon as possible, but definitely before **Thrusday noon** because after that time I'm going to compile the list.
- The key list, and a PGP (or GnuPG) keyring export will be available for your convenience at the following URL: http://people.apache.org/~jfclere/2019EUKeyring/

What is a PGP Key Signing?

This is an opportunity for committers and general attendees to sign each other's PGP or GPG keys and grow our Web Of Trust.

We will try to have time both for newbies and experienced folks. Remember too that you can sign other folk's keys at any time, not just during official events. Note that we should probably save any 'how do we encourage Apache's web-of-trust' discussions or the like for another time, so we can ensure the signing party goes quickly.

Quick instructions to prepare your self for the keysigning: create a key pair, check it and send the pub key to a server:

- gpg --gen-key (*use 1 - RSA and RSA default and 4096 for the size,* **your name and email** *and comment* (some gpg version ask only for name and email) use a safe password and remember it...
- gpg --list-secret-key --keyid-format LONG "**your name**" will list the keyid and the finger print

  the ouput is some thing like:

  sec rsa2048/**CCC0F57763ED87D6** 2019-09-05 [SC] [expires: 2021-09-04]
  A27A41DD34096A1C5DFDF18DCCC0F57763ED87D6
  uid [ultimate] Jean-Frederic Clere <jfclere@apache.org>
  ssb rsa2048/1B3AADE6DF6CA671 2019-09-05 [E] [expires: 2021-09-04]

  CCC0F57763ED87D6 is the long key you have to put in the google form

  A27A41DD34096A1C5DFDF18DCCC0F57763ED87D6 is the Fingerprint you have to remember (write it) to check the during the party.

- gpg --keyserver keyserver.ubuntu.com --send-keys **CCC0F57763ED87D6**

Committers should see https://svn.apache.org/repos/private/committers/docs/pgp-key-signing.txt for details.

Some background on what a keysigning party is:

- http://www.cryptnet.net/fdp/crypto/keysigning_party/en/keysigning_party.html (how to sign using GPG)
- http://www.faqs.org/faqs/pgp-faq/ (general PGP info)
- http://wiki.apache.org/incubator/SigningReleases (how we sign Apache releases)
- http://www.apache.org/dev/release-signing.html

Committers are recommended to add their key fingerprint to https://id.apache.org/ under *OpenPGP Public Key Primary Fingerprint*. Doing that will permit your key to show up in the ASF committer keys listings under https://home.apache.org/keys/

The PGP Keysigning Event

1. Everybody gets a print-out of the key list. I will make those and have them available.
2. The key entries on the printout are numbered. All participants line up in the order of their keys.
3. The list will also be on the projection screen (assuming we get a projector, and get it to work in a timely fashion). You verify that your entry on the printout is correct: that the key ID, fingerprint and name + e-mail information match what you submitted. You also verify that your entry on the printout is the same as your entry on the screen.
4. I will call out the name of each participant, in order. When your name is called, tell all participants loudly whether your information as verified in step 3 is correct. Stand up and wave your arms if you want to, it's very important that the other participants see and hear you assert that this key is yours.
5. As participants positively verify their information, check whether their entry on the screen matches their entry on your printout. If so, you can place a check mark in the first of the two boxes at the right of your printout. Why do we do this? To make sure we all have the same list, and that the list is correct. You are verifying that I didn't make any mistakes compiling the list, or that I didn't nefariously doctor anyone's key.
6. Once everyone's key data has been verified, the fun part starts. Everybody gets up, and forms a line in the order in which you appear on the list. Once the line is formed, we'll double it: the first person in the line walks past the line until he or she ends up next to the last person, and everyone follows until we have a double line, half as long. Then, everyone makes a quarter turn so that they face the person next to them rather than the back of the person in front.

7. Now, everyone in the line is going to *identify* every other participant. Start with the person standing (conveniently) right in front of you, then move one person to the right and repeat until you have met everyone in line. The line will fold upon itself in caterpillar fashion: once you reach the end just turn around and start going to the other side (the next person you "meet" will be your neighbour). As you make positive identification of a person, you place a check mark on their line in the second box at the right of your printout. How do you identify people? That is up to you. Some folks check each other's passport or driver's license, but that means you trust the government to provide positive identification. And who trusts the government anymore these days? Some folks just know each other, or, if they haven't met before the conference, have gotten to know each other well enough to assert that they know who they are. It's really up to you, and if you can't identify the other person to your liking, don't place that checkbox and don't sign their key.
8. After everyone has met everyone else, you should have a list with a bunch of checkmarks in the right columns. Put this list in your pocket. Back in your hotel room, fetch the keyring given above. Next, pull out the list, and sign the keys that you gave two checkmarks. Finally, upload the signed key to the following two keyservers:
    - keyserver.ubuntu.com
    - pgpkeys.mit.edu
    - minsky.surfnet.nl

      Then, send the owner of the key a signed, encrypted e-mail telling them that you have signed their key. Hopefully they will do you the same favor.

What you should bring:

1. Yourself. Obviously.
2. A cookie from your lunch box
3. A pen. Bring two, so you can give one to your neighbour in line who forgot to bring one.
4. Something to identify yourself with. Your face, your voice, unique pheromone pattern, etc. The better you can convince your fellow participants that it's really you, the more signatures you will get.
5. No computer.

No computer? No. We're not running the PGP (or GnuPG) program at the Keysigning Event, and we're not actually signing keys at the event. You're standing in line, juggling paper, pen and your beverage of choice... no way you can manipulate a computer while that's going on. And you want to be paying attention too, especially during the key verification phase. So, no Slashdotting either. Don't worry, it'll be OK. We all spend too much time with our computers anyway.

This ends the PGP Keysigning event.

The Actual Signing of Keys

Notice anything conspicuously absent from the Keysigning Event? Right, no keys are actually signed at the event. The event is purely meant to verify participants identities and to connect persons to keys. After the event, you sit at your computer, with your list of fingerprints, and sign the keys of everyone on the list whose identities you verified. Then, mail the signed keys back to their owners. You could upload a signed key to your favorite keyserver and hope the owner finds it, but mailing it directly back to them is much more straightforward. And it may prompt the other person to return the favour.

One final note: everyone has their own criteria for signing keys. Some people are fairly lax, and will sign anyone's key that they've met, or even just exchanged regular emails with. Other folks will only sign keys when they can prove your identity, or will use your key to send you a couple of messages over a period of time to verify that you use it. So don't be offended if someone doesn't sign your key immediately after the event.

Organizing a PGP Keysigning Event

All the code and the corresponding docs are on github.