# About package PGP signatures

› Table of contents

To increase confidence in the npm public registry, we add our PGP signature to package metadata and publicize our public PGP key on Keybase. Our Keybase account is "npmregistry" and our public PGP key can be found at https://keybase.io/npmregistry/pgp_keys.asc

You can use the package PGP signature and our public PGP key to verify that the same entity who published the key (npm) also signed the package you downloaded from the npm public registry. For more information, see "Verifying the PGP signature of a package from the npm public registry".

## Tools we use

### openpgpjs

To generate PGP signatures, we use openpgpjs, a pure JavaScript implementation of OpenPGP. To learn more about openpgpjs, see https://openpgpjs.org/.

### Keybase

We use Keybase to publicize our PGP key and give you confidence that the npm registry you install from is the same registry that signs packages.

Keybase offers two advantages over the core OpenPGP experience that move us to recommend it to you:

- The Keybase application and CLI provide an excellent user experience for PGP, which can be intimidating for newcomers.
- Keybase manages and displays social proofs that the entity that controls a specific PGP key also controls accounts on social media and other places. These proofs help you determine whether you can trust an account.

We've established proofs on Keybase that we control @npmjs on Twitter, the domain npmjs.com, and the domain npmjs.org. Verifying these proofs won't tell you who owns those domains, but it does establish that the same entity controls them and the PGP key advertised on Keybase.

If you install Keybase and create an account, you can follow npmregistry yourself and obtain a local copy of the registry’s public key. For more information, and to verify the PGP signature of a specific package version from the npm public registry, see "Verifying the PGP signature for a package from the npm public registry".