Verifying the PGP signature of a package from the npm public registry

Table of contents

To ensure the integrity of a package version you download from the npm public registry, you can manually verify the PGP signature of the package.

Note: Since fully verifying signatures on Keybase requires rechecking proofs (which requires network activity) and is therefore expensive, we recommend only verifying signatures if it is absolutely necessary -- for example, when verifying a deploy artifact, or when initially storing a package in your cache.

Prerequisites

1. Install Keybase from https://keybase.io/download
2. Create a Keybase account on https://keybase.io
3. Follow "npmregistry" on Keybase.
4. Download a local copy of the npm public registry's public PGP key.

Verifying npm signatures for the public registry

Note: The following steps use version 1.4.3 of the `light-cycle` package as an example.

1. On the command line, fetch the signature for the package version you want and save it in a file:

```
$ http GET https://registry.npmjs.org/light-cycle | json "versions['1.4.3'
```

2. Get the integrity field for that version (example below includes response):

```
$ http GET https://registry.npmjs.org/light-cycle | json "versions['1.4.3'
```

Example response:

```
sha512-sFcuivsDZ99fY0TbvuRC6CDXB8r/ylafjJAMnbSF0y4EMM1/1DtQo40G2WKz1rBbyiz
```

3. Construct the string that ties the unique package name and version to the integrity string (example below includes response):

```
$ keybase pgp verify --signed-by npmregistry -d sig-to-check -m 'light-cyc
```

Example response:

```
▶ INFO Identifying npmregistry
✓ <tracked> public key fingerprint: 0963 1802 8A2B 58C8 4929 D8E1 3D4D 5B12 0276
You last followed npmregistry on 2018-04-10 21:21:57 PDT
✓ <tracked> admin of DNS zone npmjs.com: found TXT entry keybase-site-verificatio
✓ <tracked> "npmjs" on twitter: https://twitter.com/npmjs/status/9812885488452403
✓ <tracked> admin of DNS zone npmjs.org: found TXT entry keybase-site-verificatio
Signature verified. Signed by npmregistry 7 minutes ago (2018-04-13 15:00:37 -0700
PGP Fingerprint: 096318028a2b58c84929d8e13d4d5b120276566a.
```