Style guide: Level AAA - Highest requirements

The highest level of UI recommendations includes adding attestation information and/or links in an available sidebar section of a registry site or platform as well as a new security page, tab or section (depending on the platform architechture). The sidebar content can link to this security content when interacted with by users seeking more detailed information.

Security page section
Having a separate, dedicated security section or page was the UI design that tested best across all user personas. Security Experts, Pragmatic Developers, and Incidental Users all found that a dedicated security page was the best place to locate the information they expected when looking for “information that helps them make a secure and safe choice about the packages they use.” This included attestation information.

Users admitted that, during their typical workflows, the security section is not their first stop when gathering information; instead, they usually begin with the general package description, source repository links, and social proof metrics. However, the security section became easily recognizable once they were ready to review security and safety-related information. This meant users were not left guessing whether they were in the right place for security details about a package or build. When such information was placed on the main registry or platform pages, users had to do extra cognitive work to determine what attestations and related data meant in that context. They spent critical seconds scanning attestation statements and asking themselves, “Where am I, and what is this information in relation to exactly?” Within a dedicated security page or section, that effort was eliminated.

Several users also noted that having a security page gave them the impression that the registry/platform and package were “serious and committed” to security. It also allowed for additional information to be included, in case more security details or advice needed to be added in the future.

Style guide: Level AAA - Highest requirements

Some registries and platforms will not have pages or tabs where a dedicated security page can be added. In these cases, as with the example of the RubyGems package below, adding a security section beneath other sections is sufficient to set it apart and provide a link from sidebar content. Further details are provided in subsequent sections about how security page sections were tested and user rationale.

SECURITY:

RubyGems.org is a repository for distributing packages, not a service for auditing them. RubyGems cannot guarantee the quality or security of the code within any given gem.

More information on gem security >

BUILD PROVENANCE (PACKAGE ORIGIN):

Source

Source: github.com/ruby/rake >

Source commit: github.com/ruby/rake/commit/0fdacef47aa9a4140e472b0ce302a... >

Build

Build file: github.com/ruby/rake/actions/runs/153403429... >

Build logs: github.com/ruby/rake/actions/runs/153403429... >

Integrity

SHA 256 checksum

96f5092d786ff412c62fde76f793cc0541bd84d2eb579caa529aa8a059934493

More on how to verify an attestation >

Attestation

RubyGems verifys that this gem file, at this checksum, was uploaded to RubyGems by GitHub Actions, using the source and build instructions detailed above.

Signed by: RubyGems on gem publication

View Full Transparency Log >

Attestations provide a trail of evidence for a gem's provenance origin.

Find out more about attestations >

INTEGRITY:

You can use checksums to verify that the file you download is exactly the same as the one hosted on RubyGems.

SHA 256 CHECKSUM:

96f5092d786ff412c62fde76f793cc0541bd84d2eb579caa529aa8a059934493

Find out how to use checksum to verify package integrity >

PROVENANCE:

Built and signed on

GitHub Actions

Build summary

Source Commit ruby/rake@0fdacef >

Build File .github/workflows/push_gem.yml >

transparency log entry >

SECURITY ADVISORIES

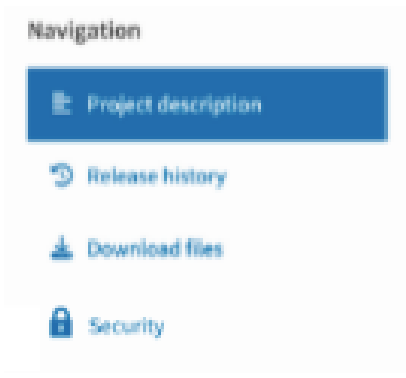
0 known advisories | **Latest:** Posted by RubySec August 29th, 2019 | **Severity:** Low

Please note: If a package has no security advisories this does not mean that there are not any vulnerabilities in this package. Please use with caution.

Source: RubySec Database >

← PREVIOUS VERSION

Style guide: Level AAA - Highest requirements



With registries or platforms like PyPI that have a left-hand menu, the security page can be added there.

PyPI is a complex example, as there is a lot of different information that users in testing considered to be "security" information that could be included in this section. The best advice is that platforms should make informed decisions about what existing information moves to the security page and what information should be linked from the security page.

Security

PyPI is a repository for distributing packages, not a service for auditing them. PyPI does not guarantee the quality or security of the code within any given package.

More information on PyPI security

Build Provenance (package origin)

Source

Source: github.com/pypa/pip

Source commit: github.com/pypa/pip/tree/2e05cae3da2cfafa6dce58167a25b7db...

Build

Built file: github.com/pypa/pip/blob/HEAD/.github/workflows/release.yml

Build logs: github.com/pypa/pip/blob/HEAD/.github/workflows/release.yml

Integrity

SHA 256

96f5092d786ff412c62fde76f793cc0541bd84d2eb579caa529aa8a059934493

More on how to verify an attestation

Attestation

PyPI verifys that this file, at this checksum, was uploaded to Pypi by GitHub Actions, using the source and build instructions detailed above.

Signed by: PyPI on pip publication

View Full Transparency Log

Attestations provide a trail of evidence for a package's origin.

Find out more about attestations

The following attestation bundles were made for `pip-25.2.tar.gz`:

Publisher: `release.yml` on pypa/pip

Attestations:

Values shown here reflect the state when the release was signed and may no longer be current.

- Statement:
  - Statement type: `https://in-toto.io/Statement/v1`
  - Predicate type: `https://docs.pypi.org/attestations/publish/v1`
  - Subject name: `pip-25.2.tar.gz`
  - Subject digest: `5782b3f006390f85bb6282dffb876454593d637f5d1be494b5202ce4877e71f2`
  - Sigstore transparency entry: 332654865
  - Sigstore integration time: Jul 30, 2025, 10:50:11 PM

Source repository:

- Permalink: `pypa/pip@2e05cae3da2cfafa6dce58167a25b7dba4bc2a33`
- Branch / Tag: `refs/tags/25.2`
- Owner: https://github.com/pypa
- Access: `public`

Publication detail:

- Token Issuer: `https://token.actions.githubusercontent.com`
- Runner Environment: `github-hosted`
- Publication workflow: `release.yml@2e05cae3da2cfafa6dce58167a25b7dba4bc2a33`
- Trigger Event: `push`

Integrity

You can use checksums to verify that the file you download is exactly the same as the one hosted on PyPI.

Algorithm	Hash digest	
SHA256	`5782b3f006390f85bb6282dffb876454593d637f5d1be494b5202ce4877e71f2`	Copy
MD5	`6d109857fa69274dacfc1d6528471eb5`	Copy
BLAKE2b-256	`2016650289cd3f43d5a2fadfd98c68bd1e1e7f2550a1a5326768cddfbcedb2c5`	Copy

See more details on using hashes here.

Security Advisories

The PyPIsec database is the central, community-maintained repository of all publicly disclosed security advisories for PyPI.

0 known advisories | **Latest:** Posted by RubySec August 29th, 2019 | **Severity:** Low

Please note: If a package has no security advisories this doesn't mean that there are not any vulnerabilities in this package. Please use with caution.

Source: The PyPISec Database

Attestations style guide

Style guide: Level AAA - Highest requirements

Security

With registries or platforms like npm that have a navigation tab bar, the security page can be added there.

In the npm examples we tested, the packages often displayed entire READMEs, which meant many pages of scrolling to find any information not included in the README. In some cases, users were confused about which information was written by package maintainers and which was provided by the registry. One suggestion that was offered, but not explored in the UI, was to add author names to content, including the publish date. For example: “This security page was last updated on [DATE] by npm to include [DETAILS].”

Security

npm is a registry for distributing packages, not a service for auditing them. npm does not guarantee the quality or security of the code within any given package.

More information on npm security

Build Provenance (package origin)

Source

Source: github.com/axios/axios

Source commit: github.com/axios/axios/tree/b76c4ac6f871141dd...

Build

Built file: github.com/axios/axios/actions/runs/164628525...

Build logs: github.com/axios/axios/actions/runs/164628525...

Integrity

SHA 256 checksum

2c3bf6b3ad073a27ec48bc36338a173a20513c3aa3d225fa5deec8bd0163b2a0

More on how to verify an attestation

Attestation statement

npm confirms that this package, at this audited using npm audit, was uploaded to npm by GitHub Actions, using the source and build instructions detailed above.

Signed by: github on build and verified by npm on upload

View Full Transparency Log

Attestations provide a trail of evidence for a packages's provenance (origin). Find out more.

Built and signed on
GitHub Actions
View build summary

Source Commit	github.com/axios/axios@b76c4ac
Build File	.github/workflows/publish.yml
Public Ledger	Transparency log entry

Integrity

You can use this command to verify that the file you download is exactly the same as the one hosted on npm.

```
npm audit signatures
```

This command checks the registry signatures and provenance attestations. If a package has missing or invalid signatures or attestations, it returns an error. This could indicate that a package has been tampered with.

Note: In order to run the audit command to verify package provenance, you must:

- Install npm CLI version `v9.5.0` or later: `npm install -g npm@latest`
- Install dependencies with `npm install` or `npm ci`

Find out how to use audit commands and 256 SHA checksum to check hashes/signatures

Security Advisories

The npmsec database is the central, community-maintained repository of all publicly disclosed security advisories for npm.

0 known advisories | **Latest:** Posted by RubySec August 29th, 2019 | **Severity:** Low

Please note: If a package has no security advisories this doesn't mean that there are not any vulnerabilities in this package. Please use with caution.

Source: npmSec Database

Style guide: Level AAA - Highest requirements

Sidebar - Minimal
If present on a page, the sidebar typically already contains critically useful information to help users decide whether or not to use a package and/or if a package is safe. This is usually where downloads, releases, source code or repository links, and contributors are listed. These pieces of information are important not just for safety and security, but are generally useful for users when exploring packages.

The sidebar also became the primary location where users wanted to see attestation information. However, users indicated that they did not want attestation or security content to push down the other important information. They were also unlikely to read detailed or lengthy text content in sidebars.

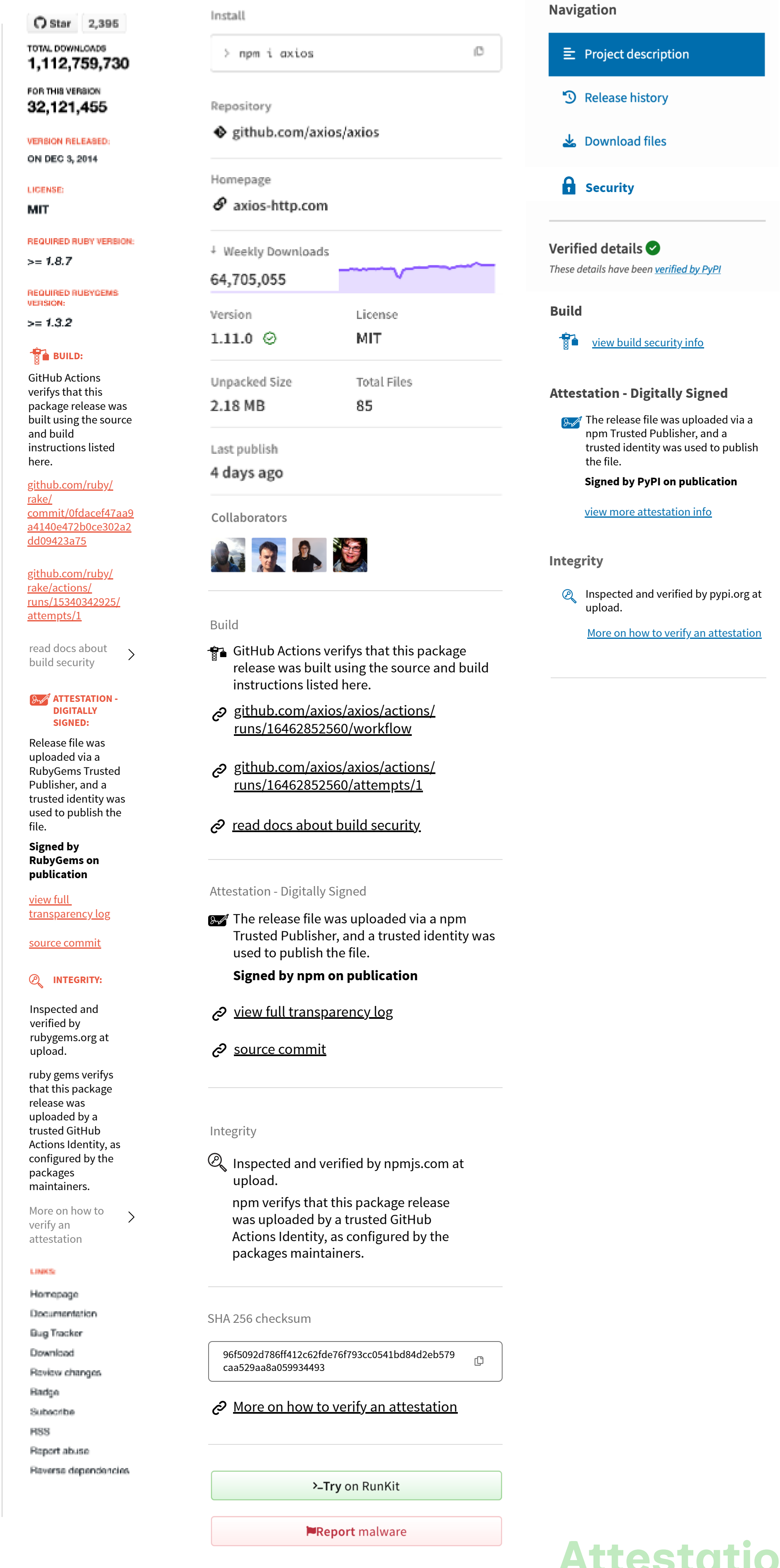
A minimal sidebar should therefore only be used in conjunction with a dedicated security page or section, with sidebar links functioning like "bookmarks" for the related security information on the page, directing or focusing the user on the relevant section when clicked (e.g., when the sidebar "Build confirmed" is clicked, it should focus on the "Build confirmed" section in the security page). In rare cases, components styled to meet Level AA requirements can be used optionally here in the UI alongside the minimal sidebar.

Sidebar - Maximum
The maximum sidebar is a UI designed for users who are unlikely to explore the security page and do not want to dive deeply into security information or be redirected there by a link in the sidebar. These users are relatively rare, as the general expectation for sidebars is to contain only a few words of text (certainly not full sentences). However, there are scenarios where registries or platforms may want to display as much information in the sidebar as possible, or include some of the content from the security page as well.

Style guide: Level AAA - Highest requirements

See below dedicated security sections, nav bar tabs and left hand menu tabs. We tested the term 'security with and without the lock icon and it was preferred with the lock icon as so to reenforce user understanding of what this section does. it was not confused with a 'locked' section.

There may be cases where the visual style of a regitry or platform does not allow for icon usage. it is acceptable to omit the lock icon in these cases.



Attestations style guide

Style guide: Level AAA - Highest requirements

As previously stated, when positioning attestation content in the sidebar, it should not appear above essential general information such as:

- Source code repository links
- Homepages/URLs (if applicable)
- Releases
- License
- Download numbers (weekly, etc.)
- Version number
- File size
- Last published date
- Maintainer/Contributor profile pictures and/or names

Typically, this means that attestation information will still appear within the first scroll of the sidebar. Ideally, it should be placed as high as possible without displacing essential information.

We tested some expandable sections in the sidebar, but these did not perform well with users. There is a general expectation that sidebar information should be presented as is, or take you to an internal or external link, rather than expanding or contracting within the sidebar.

Generic webpage structure