

Style guide: Level AA – Medium

This section of the style guide defines the medium (Level AA) requirements for displaying attestation information on package registries, aiming to strengthen users' sense of security and trust in a package's build integrity.

Package repositories opting to implement these recommendations will need to allocate more visual space within their user interfaces. This approach expands upon the information introduced in the lowest (Level A) requirements by proactively revealing additional details, source links, and clear pathways for users to explore and better understand attestation and related information.

There are variants for medium-level requirements:

1. **Three-Card Layout:** Information is presented in distinct "cards" or modules. Each card includes icons, headings, labeled source links, and links to documentation (where relevant). This variant typically features three cards, with flexibility for additional cards as needed.
2. **Four (Larger) Card Layout:** Designed for package registries with more visual space, this variant utilizes larger card designs. It typically features four cards, with flexibility for additional cards as needed.

During user testing, we found that variants one and two (three card and four card layouts) were most effective in helping users explore the safety, security and integrity of a package, along with the included links.

User research notes from this project, please see:

• <https://github.com/ossf/wg-securing-software-repos/issues/66>

Notes from user tests focused on evaluating attestation user interfaces for clarity and user preference.

Style guide: Level AA - Medium requirements



Source

Source repo: github.com/ruby/rake

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



Build confirmed

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

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



Attestation Signed

RubyGems confirms that this gem file was uploaded to RubyGems by GitHub Actions.

Signed by RubyGems .org on publication

[View Transparency log](#)



Source

Source repo: github.com/axios/axios

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



Build confirmed

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

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



Attestation Signed

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

Signed by: npm on publication

[View Transparency log](#)



Source

Source repo: github.com/pypa/pip

Source commit: github.com/pypa/pip/tree/2e05cae3da2cfafa6dce58167a25...



Build confirmed

Build file: github.com/pypa/pip/blob/HEAD/.github/workflows...

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



Attestation Signed

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

Signed by: PyPI on pip publication

[View Transparency log](#)

The detail here is the same as the expanded version of the minimal, Level A component. Differences are that the package name, version number and box icon has been swapped with a browser and code brackets icon with the heading of "Source". To users, the package icon, name and the source icon and label source mean the same/ similar enough terms and the associating information of repo and source commit contextualise the heading for them.

Later in this style guide we'll clarify the use of the terms like "build confirmed" versus the use of "verification".

Again, the Build Confirmed card contains the build commit (for the version available on the page/ platform) and the build logs. Please note these example links may not be exactly accurate link destinations.


The Transparency log link can either be the URL or a hyperlink. More detail about hyperlinks can be found in the hyperlinks page of this style guide.

Box width = 200px Height = 160px in example

Cards are designed so that three should fit in most main page widths for platforms and boxes can be stacked e.g. if there are two or more attestations the fourth box can go below the Source card etc.


Attestations

Style guide: Level AA – Medium requirements

**Build confirmed**

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


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

**Attestation Signed**

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


Signed by RubyGems.org on publication

Transparency log: search.sigstore.dev/?logIndex=225255766

**Source**


Source repo: github.com/ruby/rake

Source commit: github.com/ruby/rakecommit/0fdacef47aa9a4140e472b0ce302a2dd09423a75

**Integrity**

SHA 256 checksum

96f5092d786ff412c62fde76f793
cc0541bd84d2eb579caa529aa8
a059934493



[More on how to verify an attestation](#)

Box width = 260px Height = 200px in example

Again, these cards are designed to be stacked and so that two should fit within the width of the main content area of standard page layouts. For example, if there are two or more attestations they can form a row of two: the Source card can go next to the Build Confirmed card, and the Integrity card can occupy a single space with an empty space next to it, or be centered in the layout to suit tastes.

These cards contain the same information as the version on the previous page with three cards in a row. The only notable difference is that, with more space, the Transparency Log label and link can be gently sectioned off with a dotted line to maintain its association with the attestation while also occupying its own distinct space.

By having two (or three, depending on page width) cards horizontally, with others stacked below, we can introduce more supporting information near the attestation box. The Integrity card should contain the "checksum" used to verify the attestation, along with a link to documentation to inform and educate users. Checksums are explored in more detail in this style guide.

The possible and likely scenario of checksums being duplicated across page information is also addressed in the large medium UI mockups. In short, duplication was not an issue for users across any links or information. In fact, repeating details—such as links or checksum details, when they are supposed to match—was seen as a positive. All users we tested with reported greater confidence in the validity of the entire page's information as a result.

Style guide: Level AA - Medium requirements



Build confirmed

Build file: [github.com/axios/axios/
actions/runs/164628525...](https://github.com/axios/axios/actions/runs/164628525...)

Build logs: [github.com/axios/axios/
actions/runs/164628525...](https://github.com/axios/axios/actions/runs/164628525...)



Attestation Signed

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

Signed by: npm on publication

Transparency log: [search.sigstore.dev/?
logIndex=304840876](https://search.sigstore.dev/?logIndex=304840876)



Source

Source repo: github.com/axios/axios

Source commit: [github.com/axios/axios/tree/
b76c4ac6f871141dd...](https://github.com/axios/axios/tree/b76c4ac6f871141dd...)



Integrity

SHA 256 checksum

96f5092d786ff412c62fde76f793
cc0541bd84d2eb579caa529aa8
a059934493




[More on how to verify an attestation](#)

An example of the larger card sizes when a page width allows for three cards in a row with an additional Integrity card stacked under them in a row by itself.


This indicates to the users that there could be more future information added here that is relevant to attestations. The design and layout did not look like there was 'unused space' to users but when implementing caution should be used when allowing for many solo/one cards as the information looks 'orphaned' when only one card is present and it does not attempt to span the width of the page layout's available space.

Style guide: Level AA – Medium requirements

**Build confirmed**


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

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

**Source**


Source repo: github.com/pypa/pip

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


**Integrity**

SHA 256 checksum

96f5092d786ff412c62fde76f793
cc0541bd84d2eb579caa529aa8
a059934493




[More on how to verify an attestation](#)

**Attestation Signed**

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

Signed by RubyGems on publication

Transparency log: search.sigstore.dev/?logIndex=225255766

**Attestation Signed**

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

Signed by RubyGems on publication

Transparency log: search.sigstore.dev/?logIndex=225255766

An example—if appropriate and if sufficient page width is available—is centering a smaller row of cards beneath a larger row, as seen here with three cards in the first row and two cards in the second row, rather than either left or right aligning the smaller row. (The example shown uses two of the same attestation and is only intended to demonstrate display orientation.)

Style guide: Level AA – Medium requirements

The positioning for the medium level AA UI are the same as the lowest level A UI.

After critical functional information about what the package does and as near to the 'social proof' information as possible aka download numbers, maintainer/contributor profiles/names and other package provenance information.

There was another tested Medium UI component that we've documented for clarity but no longer recommend implementing. This design follows in the next pages of medium requirements.

Generic webpage structure

Header/nav/logos/menus etc.


Critical informative content in first section/scroll.







Best placement for the UI for Attestations + additional info in the top of the second scroll.

Specific information rarely scanned by users.

Footer

Style guide: Level AA – Medium requirements

 **axios v 1.11.0** Created by npm/axios, Built and signed by GitHub Actions, verified by npm

 Source Source repo: github.com/axios/axios Source commit: github.com/axios/tree/b76c4ac6f871141dd...  Limitation This attestation verifies the gem source, but does not certify the security of the underlying source code.	 Build confirmed Build file: github.com/axios/axios/actions/runs/164628525... Build logs: github.com/axios/axios/actions/runs/164628525...  Attestation Signed npm verifies that this package audited using npm audit, was uploaded to npm by GitHub Actions, using the source and build instructions detailed. Signed by: npm on publication search.sigstore.dev/?logIndex...	 Integrity SHA 256 checksum <div>96f5092d786ff412c62fde76f793 cc0541bd84d2eb579caa529aa8 a059934493 </div> More on how to verify an attestation Inspected and accepted by: npmjs.com at upload npm confirms that this package was uploaded to npm by GitHub Actions.
--	--	--

This variant of the card component maintains a distinct design for the registries and platforms that would like these details to look like a clearly separate component that is different (external) from regular page information. The colors and brand design elements can be styled per platform.


This version also emphasizes explanatory text and warnings about the limitations of attestations—specifically, what an attestation is versus how the information presented might be interpreted by a user.

Regarding language: this is the minimal design with the most clarifying text. For platforms that want to include as much disclaimer-like text as possible, this design (or the highest level, AAA, described later in this style guide) is recommended.






When testing this large card's design, we learned that every user coming to a package registry page has some level of caution and/or doubt about the information it contains. They already arrive cautious and with shaky trust levels. This is due to thoughts like, "Anyone can just put any text or info on these pages, right? The maintainers or the registry, anyone? So by default, I don't trust information unless I look at the sources and confirm for myself."

This means that "(!) caution..." messages—while they reinforce users' existing caution and clarify risks—are often bothersome and typically unhelpful beyond a single, simple warning that reminds users to be careful. We recommend reducing the number of warning and caution-type messages across the page.

Style guide: Level AA – Medium requirements

 **rake v13.3.0**

Created by Ruby/Rake, Built and signed by GitHub Actions, Accepted by RubyGems

 Source Source repo: github.com/ruby/rake Source commit: github.com/ruby/rake/commit/0fdacef47aa9a4140e472b0ce302a...  Limitation This attestation confirms the gem source, but does not certify the security of the underlying source code.	 Build confirmed Build file: github.com/ruby/rake/actions/runs/153403429... Build logs: github.com/ruby/rake/actions/runs/153403429...  Attestation Signed GitHub Actions confirms that this gem release, at this checksum, was built using the source and build instructions listed here. Signed by GitHub Actions at gem build search.sigstore.dev/?logIndex=22...	 Integrity SHA 256 checksum <div>96f5092d786ff412c62fde76f793cc0541bd84d2eb579caa529aa8a059934493</div> More on how to verify an attestation Inspected and accepted by: RubyGems.org at upload RubyGems confirms that this gem file was uploaded to RubyGems by GitHub Actions.
--	---	--

A note on the words “verification,” “verified,” and “verify” versus using similar words like “confirm,” “confirmed,” “accepted,” “accepts,” “validates,” “inspected,” etc.

When we asked users to explain back to us what attestation language meant to them, in our user tested designs, we avoided using 'verified' as a term and relied on confirmed/accepted as common language.


Users non proficient in attestation nuances would explain this information as 'verification of complete safety of the package'. When we clarified that verification of complete safety is aspirational and not necessarily what is on offer here, users did indicate that they know no package is 100% safe no matter what information is offered but the choice to use the words 'verification' and 'verified' should be used with caution since users are already jumping to a verified = complete safety assumption.













The language used in the card here—such as “confirms,” “accepts,” etc.—still clearly explains to users what is happening: that entities are checking details and asserting an opinionated “clearance” of certain aspects, such as build provenance or expected origin. However, users often jump to “verified!” assumptions. The term “verification” should only be used when a platform is prepared to accept the risk of users assuming full safety of a package when this word is present.

Style guide: Level AA - Medium requirements

Medium design that users least preferred.

We mixed up all designs when showing users the UI. Users received Highest first, Lowest first and Medium first. This design tested the least favourably with users and therefore we're removing from the recommendation but retaining as documentation in the style guide to ensure clarity.

 **pip v25.2** Created by PyPi/pip, Built and signed by GitHub Actions, Accepted by PyPi

 Source Source repo: github.com/pypa/pip  Source commit: github.com/pypa/pip/tree/2e05cae3da2cfafa6dce58167a25...   Limitation This attestation confirms the gem source, but does not certify the security of the underlying source code.	 Build confirmed Build file: github.com/pypa/pip/blob/HEAD/.github/workflows...  Build logs: github.com/pypa/pip/blob/HEAD/.github/workflows...   Attestation Signed GitHub Actions confirms that this release, at this checksum, was built using the source and build instructions listed here. Signed by GitHub Actions at build search.sigstore.dev/?logInd... 	 Integrity SHA 256 checksum <div>96f5092d786ff412c62fde76f793cc0541bd84d2eb579caa529aa8a059934493 </div> More on how to verify an attestation  Inspected and accepted by: PyPi at upload PyPi confirms that this gem file was uploaded to PyPi by GitHub Actions.
--	---	--

This card attempts to combine all of the most useful information tested in the more minimal light and medium versions. Short of the AAA requirements, we consider this to be the most comprehensive version of the component which introduces new pages or sections to registries and platforms. This design aims to show all of the most relevant and relational information, including the specific, essential attestation data. You could liken it to having the “nutrition label” right next to the food name.