Daniel Fett
Oliver Terbu
Brian Campbell

IETF OAuth WG
July 2025

SD-JWT VC

IETF 123 Madrid

draft-ietf-oauth-sd-jwt-vc

Quick SD-JWT VC Review/Overview

- Describes data formats as well as validation and processing rules to express Verifiable Credentials† with JSON payloads with and without selective disclosure based on the SD-JWT format
- Uses SD-JWT and the well-established JWT content rules and extensibility model as basis for representing VCs††
- Describes [SD-]JWT VC Issuer Metadata and key resolution
- Describes Type Metadata
- Does not utilize the W3C's Verifiable Credentials Data Model v1.0, v1.1, or v2.0
  - But does not prohibit such content (for example, OpenID4VP's SD-JWT VCLD happened)

† a.k.a., Digital Credentials or Verifiable Digital Credentials

†† or DCs or VDCs

Since [one night in] Bangkok: Drafts -09 & -10

-09

- Use SD-JWT KB in place of SD-JWT with Key Binding JWT
- Editorial changes
- Document reasons for not using JSON Pointer or JSON Path
- Clarify that private claim names MAY be used
- Update PID Example
- Fix section numbering in a few SD-JWT references

-10

- Fix `[...]#integrity` claim values in examples (Subresource Integrity uses regular base64 encoding and some were wrong length)
- Rename 'Issuer-signed JWT Verification Key Validation' to 'Issuer Signature Mechanisms' and rework some text accordingly. Provide a web-based metadata resolution mechanism and an inline x509 mechanism. A DID-based mechanism is not explicitly provided herein but still possible via profile/extension. Be explicit that the employed Issuer Signature Mechanism has to be one that is permitted for the Issuer according to policy. Be more clear that one permitted Issuer Signature Mechanism is sufficient.

in -10: Issuer Signature Mechanisms

- Clearly defined **extension point** for signature key validation options
- Allows for **concise definition** of signature mechanism and key resolution
- **Two common mechanisms** defined for **interoperability**:
  - web-based metadata resolution via .well-known and JWKs
  - inline x509 via x5c header
- Including security and implementation considerations
- Acceptable mechanism(s) for a given issuer are per verifier policy
- Verifying one acceptable mechanism is necessary and sufficient

did:note:
DID-based mechanism not explicitly provided, but can be defined in profile/extension

Why not DIDs?

We do not provide a DID-based Issuer Signature Mechanism predefined in the specification, mainly due to

- Complexity for implementers
  - Proliferation of 200+ DID methods not reasonably implementable for most developers
  - Profiles can provide actionable implementation guidance
- Interoperability concerns
  - “Just implement (some) DID methods” leads to non-interoperable implementations
  - Guidance should be provided in use-case specific profiles:
    - Selection of DID(s) for interoperability
    - Policies around accepting different DID methods
- Reputational risk
  - Potential damage to the credibility and perceived seriousness of a standards-track IETF document

➔ Means applications using DIDs should extend/profile/mention this specification to provide an appropriate Issuer Signature Mechanism

➔ As discussed at IETF 121 & 122, on the interim call, on the mailing list, and more

The View Ahead:

What can we accomplish before IETF 124?

winds beginning to shift

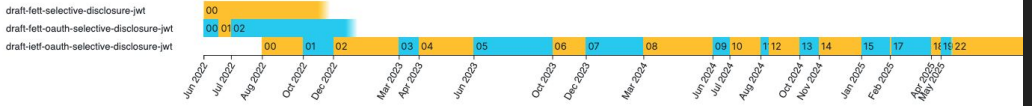
Selective Disclosure for JWTs (SD-JWT)

draft-ietf-oauth-selective-disclosure-jwt-22

Status | IESG evaluation record | IESG writeups | Email expansions | History

Versions:

00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22



Document	**Type**	Active Internet-Draft (oauth WG)
	Authors	Daniel Fett, Kristina Yasuda, Brian Campbell
	Last updated	2025-06-06 (Latest revision 2025-05-29)
	Replaces	draft-fett-oauth-selective-disclosure-jwt
	RFC stream	Internet Engineering Task Force (IETF)
	Intended RFC status	Proposed Standard
	Formats	txt html xml htmlized pdf bibtex bibxml
	Reviews	ARTART Telechat review (of -19) by Henry Thompson — Ready w/nits OPSDIR IETF Last Call review (of -19) by Tirumaleswar Reddy.K — ! Has issues ARTART IETF Last Call review (of -18) by Henry Thompson — Ready w/issues SECDIR IETF Last Call review (of -17) by Shawn Emery — ! Has nits GENART IETF Last Call review (of -17) by Thomas Fossati — Ready
	Additional resources	Mailing list discussion
Stream	**WG state**	Submitted to IESG for Publication
	Document shepherd	Hannes Tschofenig
	Shepherd write-up	Show — Last changed 2025-03-03
IESG	**IESG state**	RFC Ed Queue

OpenID FOUNDATION SPECIFICATIONS CERTIFICATION GROUPS CALENDAR Search... Sign-In

Digital Credentials Protocols (DCP) Working Group - Specifications

The goal of the Digital Credentials Protocols (DCP) working group is to develop OpenID specifications for the Issuer-Holder-Verifier-Model use-cases to enable issuance and presentations of the Digital Credentials of any format (W3C VCs, IETF SD-JWT VCs, ISO/IEC 18013-5, etc.) and pseudonymous authentication from the End-User to the Verifier.

Digital Credentials Protocols (DCP) Working Group **OVERVIEW**

Digital Credentials Protocols (DCP) Working Group **CHARTER**

Digital Credentials Protocols (DCP) Working Group **SPECIFICATIONS**

Digital Credentials Protocols (DCP) Working Group **REPOSITORIES**

Some specifications are planned to be migrated from the Connect WG and some will be adopted in the new DCP WG. For the list of anticipated work items, please reference the DCP WG Charter.

Final Specifications

- **OpenID for Verifiable Presentations 1.0:** https://openid.net/specs/openid-4-verifiable-presentations-1_0-final.html

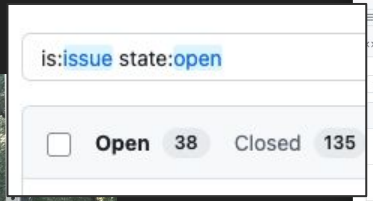
Implementer's Drafts

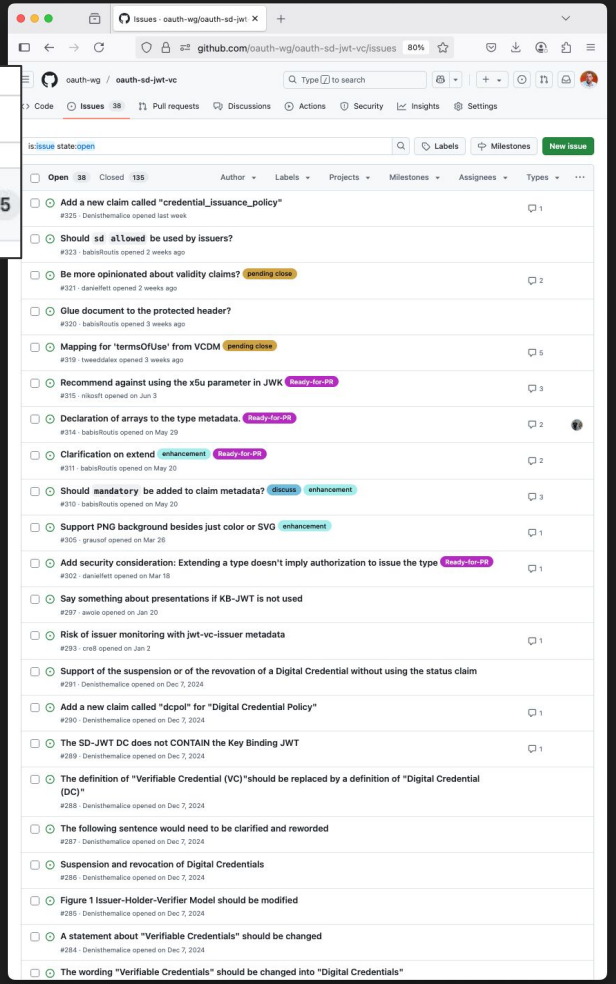
- **OpenID for Verifiable Credential Issuance (OID4VCI)**– Defines an API and corresponding OAuth-based authorization mechanisms for issuance of Verifiable Credentials
  - Editors' Draft (a version that reflects most recent changes since the last WG draft)
  - Working Group Draft
  - First Implementer's Draft (provides IPR protection to the Implementers)

Drafts

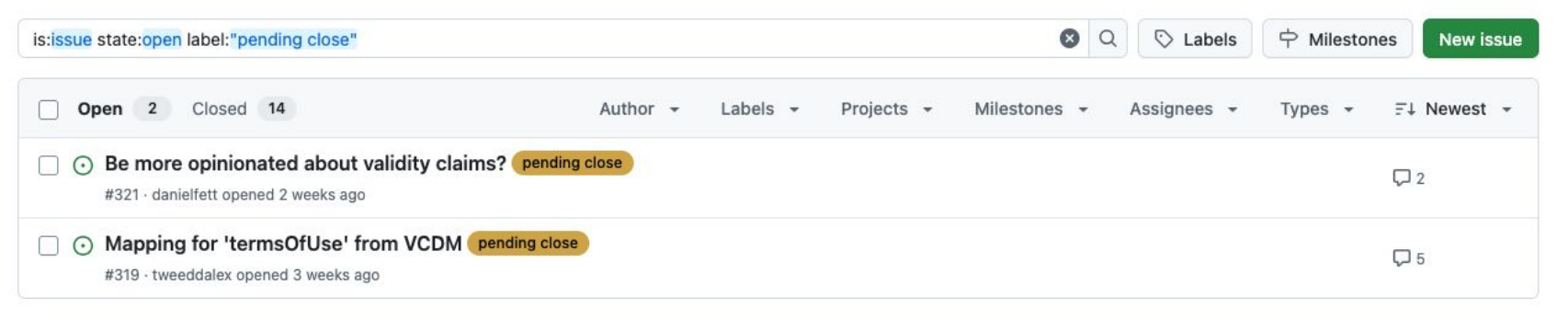
- **OpenID4VC High Assurance Interoperability Profile (HAIP)**
  Defines an profile of OpenID 4 VC for fulfilling high assurance requirements in conjunction with the SD-JWT VC or mdoc credential formats

But we're not quite





Practically free



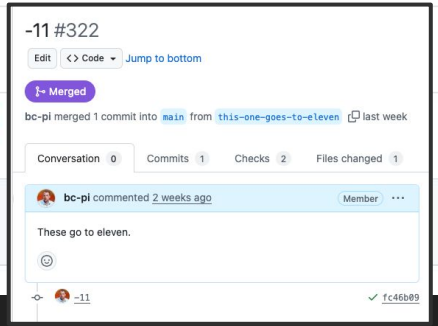
Ready Player One?

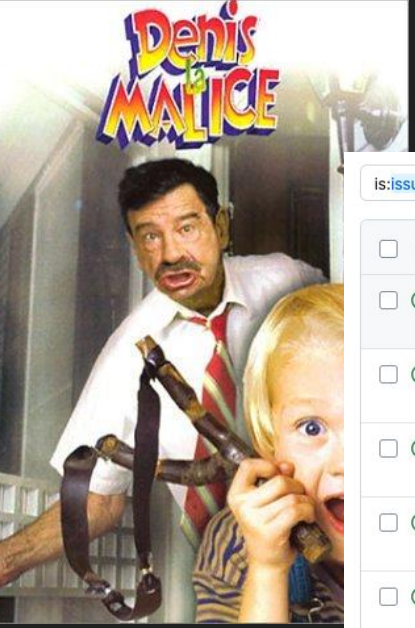
is:issue state:open label:Ready-for-PR

Labels | Milestones | New issue

Open 8 | Closed 11 | Author | Labels | Projects | Milestones | Assignees | Types | Newest

- Recommend against using the x5u parameter in JWK [Ready-for-PR] — #315 · nikosft opened on Jun 3 — 3
- Declaration of arrays to the type metadata. [Ready-for-PR] — #314 · babisRoutis opened on May 29 — 2
- Clarification on extend [enhancement] [Ready-for-PR] — #311 · babisRoutis opened on May 20 — 2
- Add security consideration: Extending a type doesn't imply authorization to issue the type [Ready-for-PR] — #302 · danielfett opened on Mar 18 — 1
- Why vct is not selectively disclosable, but vct#integrity is not? [Ready-for-PR] — #258 · Sakurann opened on Oct 7, 2024 — 4
- Add JWS JSON serialization example [Ready-for-PR] [wg-05] — #222 · awoie opened on Mar 26, 2024 — 6
- Security considerations on integrity of Type Metadata [metadata] [PRIO] [Ready-for-PR] [wg-05] — #221 · danielfett opened on Mar 26, 2024 — 2
- the wallet finding the user claims in the credential [Ready-for-PR] — #215 · Sakurann opened on Feb 27, 2024 — 7





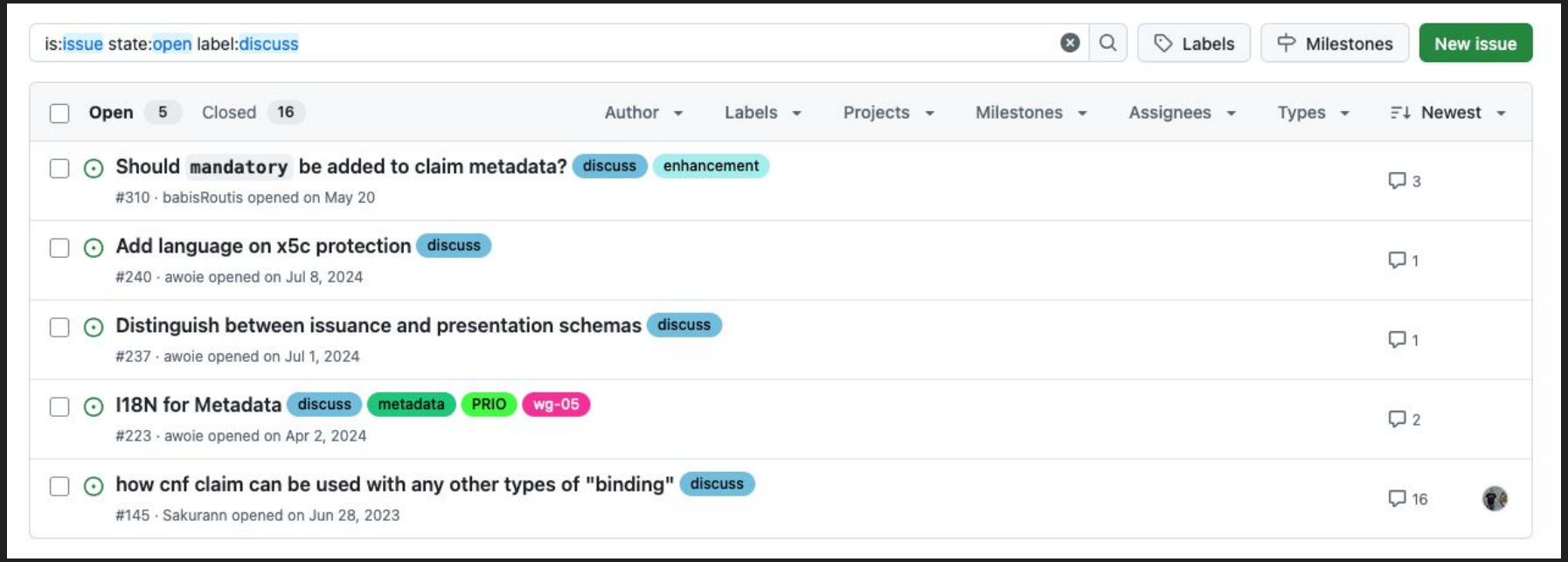
is:issue state:open no:label author:Denisthemalice

Labels | Milestones | New issue

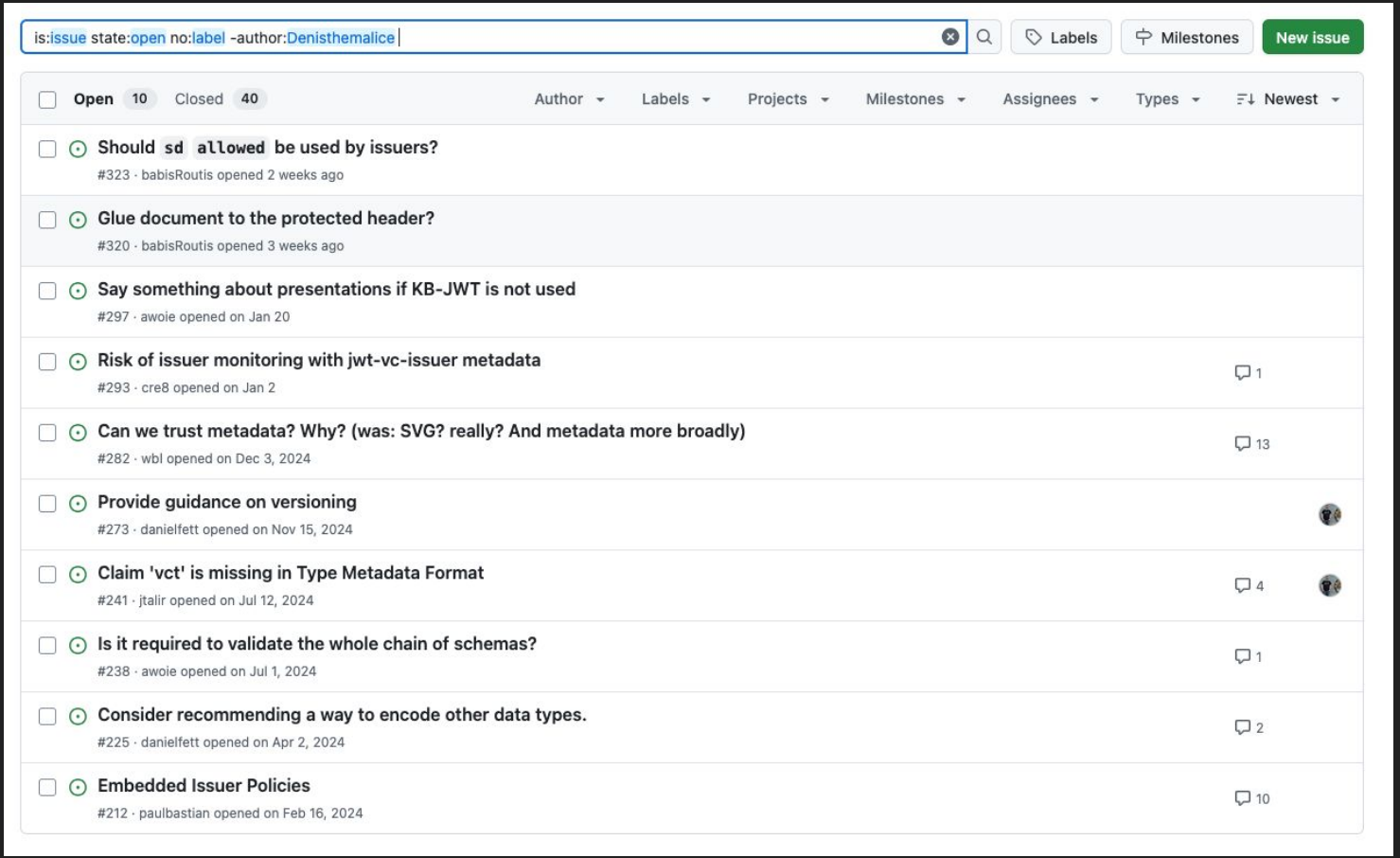
Open 10 | Closed 0 | Author | Labels | Projects | Milestones | Assignees | Types | Newest

- Add a new claim called "credential_issuance_policy" — #325 · Denisthemalice opened last week — 1
- Support of the suspension or of the revovation of a Digital Credential without using the status claim — #291 · Denisthemalice opened on Dec 7, 2024
- Add a new claim called "dcpol" for "Digital Credential Policy" — #290 · Denisthemalice opened on Dec 7, 2024 — 1
- The SD-JWT DC does not CONTAIN the Key Binding JWT — #289 · Denisthemalice opened on Dec 7, 2024 — 1
- The definition of "Verifiable Credential (VC)"should be replaced by a definition of "Digital Credential (DC)" — #288 · Denisthemalice opened on Dec 7, 2024
- The following sentence would need to be clarified and reworded — #287 · Denisthemalice opened on Dec 7, 2024
- Suspension and revocation of Digital Credentials — #286 · Denisthemalice opened on Dec 7, 2024
- Figure 1 Issuer-Holder-Verifier Model should be modified — #285 · Denisthemalice opened on Dec 7, 2024
- A statement about "Verifiable Credentials" should be changed — #284 · Denisthemalice opened on Dec 7, 2024
- The wording "Verifiable Credentials" should be changed into "Digital Credentials" — #283 · Denisthemalice opened on Dec 7, 2024

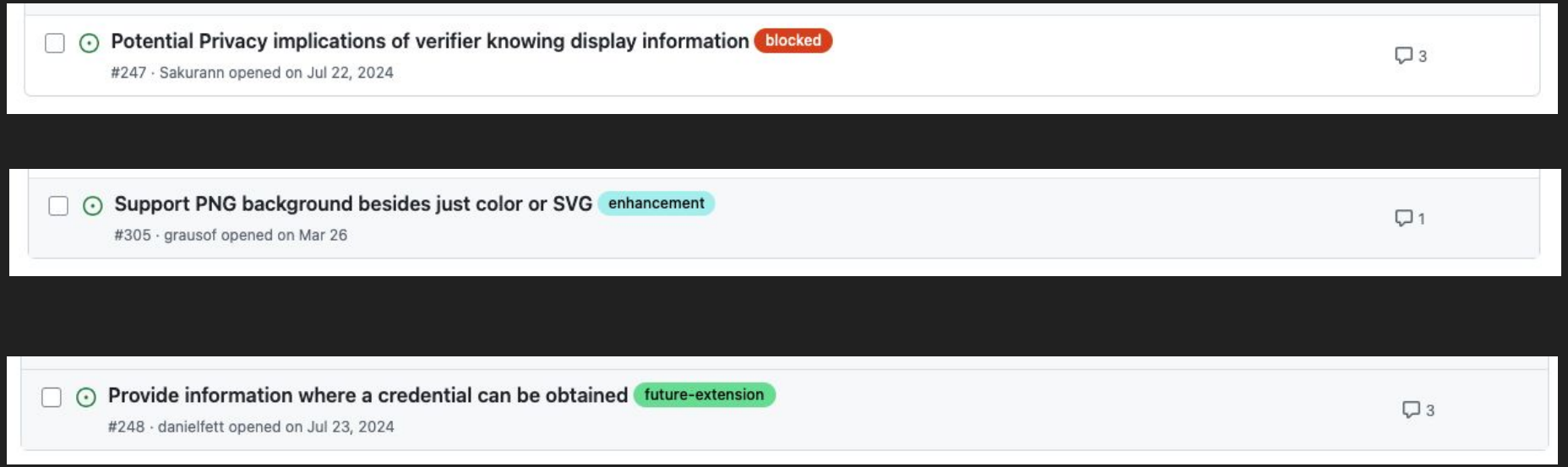
discuss isn’t DISCUSS



Others receiving no label



Island of Misfit Toys



Let’s get to work!

Monument to the Unknown ~~Bureaucrat~~ Technocrat