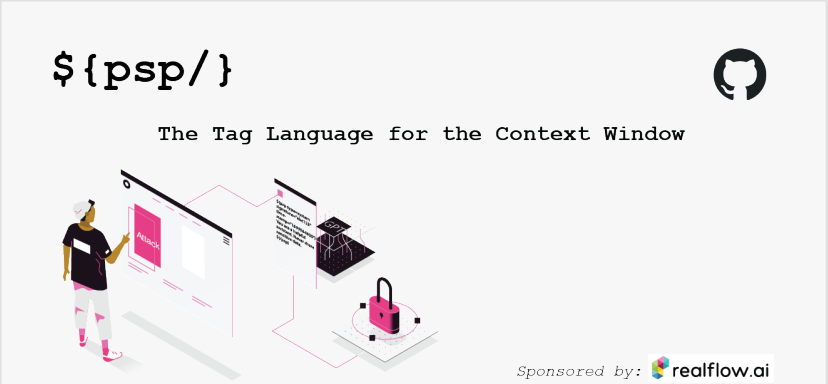
Realflow.ai Releases Prompt State Protocol (PSP) for LLMs as Open Standard Under Apache 2.0 License

First open specification that enables AI workflows directly in the context window while addressing critical prompt injection vulnerabilities.

HOUSTON, TX, NY, UNITED STATES, December 9, 2025 /EINPresswire.com/ -- Realflow.ai Releases Prompt State Protocol (PSP) as Open Standard Under Apache 2.0 License
First open specification that enables AI workflows directly in the context window while addressing critical prompt injection vulnerabilities



PSP The embedded tag language for the context window.

realflow.ai

Realflow.ai Logo

Energy LIVE 2025 Conference - Realflow.ai today announced the public release of the Prompt State Protocol (PSP) specification under the Apache 2.0 license, making enterprise-grade AI workflow orchestration and prompt security freely available to developers, researchers, and organizations worldwide.

PSP represents a new approach to building AI-powered applications. Rather than requiring external orchestration engines or custom programming, PSP enables complete business workflows to execute directly within an AI model's context window-guided by cryptographically signed instructions that the model reads and follows like natural language.

> We're not claiming to have solved prompt injection, but PSP moves the defense to a cryptographically-secure layer."
>
> *Mick Seals, CTO*

"Think about how a good business conversation works," said Mick Seals, Founder and CEO of Realflow.ai. "A single thread runs through it. You don't jump randomly between

topics-there's a natural flow from discovery to decision to action. PSP brings that same structure to AI interactions. It helps guide business conversations along defined paths while maintaining focus, even across multiple sessions or human approval steps."

Addressing the Prompt Injection Challenge

Prompt injection-where malicious input manipulates AI system instructions-remains the top security vulnerability in AI applications according to OWASP. PSP addresses this through cryptographic signatures that create verifiable trust boundaries. System instructions are signed and timestamped, allowing AI models to distinguish between trusted governance rules and untrusted user input.

"We're not claiming to have solved prompt injection," Seals noted. "But PSP moves the defense from the semantic layer-where attacks consistently succeed by rephrasing-to the mathematical layer, where cryptographic verification provides deterministic protection."

Zero Trust

We have found a way for the LLM to recognize when an attacker is trying to use agents in an inappropriate way. We default to zero trust and then allow individual steps in the conversation (we call them nodes) to be associated with only the agents it may need.

Workflows Without the Wiring

Beyond security, PSP introduces a fundamentally different way to build AI applications. Traditional approaches require developers to write orchestration code that drives the AI step by step. With PSP, the AI model itself becomes the orchestration engine, reading workflow definitions as natural language and executing them autonomously.

This enables business analysts and domain experts to define sophisticated multi-step processes-complete with decision points, human approvals, and external integrations-without writing code. The same PSP workflow runs unchanged across Claude, GPT, Gemini, or any capable model.

Open Standard, Commercial Services

The complete PSP specification is available immediately at realflow.ai under Apache 2.0 licensing. Organizations can implement PSP in their own infrastructure at no cost.

Realflow.ai will follow this release with a complete SaaS platform scheduled for January 1, 2026, offering:

- Visual workflow builders for creating PSP applications
- Hosted signing API services with key management
- MCP servers for signature verification and workflow persistence
- Pre-built connectors for enterprise systems
- Human-in-the-loop approval workflows with expiring links and notifications

---

Get Started Today

• Download the Specification: Full RFC documentation available at https://github.com/realflowmick/psp
• Try It Now: Download the sample system prompt, an example PSP workflow, sign it, and run it.
• Register for Whitepapers: Technical deep-dives on PSP architecture and implementation patterns
• Join the Early Access Program: SaaS platform access granted first-come, first-served beginning January 1, 2026

To register your interest and receive whitepapers, visit realflow.ai/early-access.
We are excited to see what you build!

About Realflow.ai
Realflow.ai is building governance-first AI infrastructure for the enterprise. Founded by Mick Seals, a 40-year veteran of enterprise consulting, Realflow.ai develops open standards and commercial services that enable organizations to deploy AI applications with confidence. The company is headquartered in Houston, Texas.

Media Contact
Mick Seals
Founder & CEO
https://realflow.ai
press@realflow.ai

Mick Seals
Realflow.ai
+1 315-359-9198
mick@realflow.ai
Visit us on social media:
X
