

Can consent become a type system for agents?

Abstract. PCHP names identity, purpose, exact scope, validity, delivery, and receipt. The hard engineering question is whether those properties can become machine-checkable invariants across tool calls, instead of natural-language promises around them.

THE PROBLEM

How should scope, purpose, expiry, subject, and revocation compose so an agent cannot accidentally widen a grant while planning a multi-tool task?

HARD CONSTRAINTS

- 01 A published registry and a token mint must share one vocabulary.
- 02 Action tools must fail closed; read tools must not become covert write paths.
- 03 Receipts must make a decision explainable without storing the private payload.
- 04 Cross-device state cannot be honestly claimed before it has a durable, revocable model.

A FIRST CONTRIBUTION

Build a small, typed grant algebra and a property-based test suite: no composed plan may execute outside the intersection of its active grants.

BUILD IN THE OPEN

github.com/hushh-labs/hushh-research
hushh.ai/discord

