

When an AI agent acts for your customer, can you prove they authorized it?

Cryptographically verifiable Digital IDs that bind every agent action to a real, verified human.

THE SITUATION

Every major agentic commerce framework defines what a credential can do. None of them specify who verifies the human behind it, which leaves the issuance layer open at exactly the point where disputes get settled.

The FBI's IC3 logged \$17.7 billion in cyber-enabled fraud losses in 2025 across 452,868 complaints. Agents raise the volume and the speed of the same attacks, and an activity log is not evidence that anyone authorized anything.

Proof issues cryptographically verifiable Digital IDs a person owns and presents again without starting over. Every use produces a signed record, including when an AI agent acts on their behalf.

WHAT THE RECORD CARRIES

- 01 Who authorized the action, bound to a verified person
- 02 What was authorized: the action, the counterparty, the ceiling, the time window
- 03 When it happened, cryptographically signed at the moment of use
- 04 Whether a person or an agent acting for them submitted it

USE CASES



Account recovery and the support desk

A caller reaches your support desk claiming to be locked out. KBA and a callback number are what stand between an attacker and the account. A reusable Digital ID lets the real customer re-prove identity in seconds, and leaves a signed record of who took the action.



Agent-initiated transactions

A customer's AI assistant opens an account, buys a policy, or files a claim. Your logs show the request arrived and succeeded. x401 lets the service ask that agent to present proof of who authorized the action, within a scope the customer set, before access is granted.

CRYPTOGRAPHIC PROOF, NOT A RISK SCORE

Most identity verification compares a document to a selfie and returns a probability that the two match. That probability is useful, and it is a different thing from proof. Proof issues a credential the person cryptographically owns, verified mathematically rather than inferred. Document authentication, biometrics, and liveness feed that enrollment rather than compete with it.