



DigiCert® AI Agent Trust

AI agent identity, security, and governance.

AI agents are rapidly becoming part of the enterprise workforce, accessing critical systems, handling sensitive data, and making autonomous decisions at machine speed. Yet most organizations lack the visibility, governance, identity, and security controls needed to manage these agents with confidence. Shadow AI is everywhere, creating significant security, privacy, and compliance risks.

There is a better way to establish trust in AI agents.

DigiCert AI Agent Trust delivers a unified trust framework that enables organizations to discover AI agents, establish cryptographic identities, enforce least-privilege access, and govern agent behavior. By combining workload identity, trusted service discovery, policy-based authorization, lifecycle management, and immutable audit trails, DigiCert enables organizations to ensure every AI agent is authenticated, authorized, accountable, and operating within clearly defined guardrails.

AI agents are the new digital workforce. And yet most organizations can't see the agents already in production and aren't prepared to secure or govern them.

98%

of organizations have employees using unsanctioned AI

[Netskope](#)

13%

of organizations say they are prepared to manage AI agents at enterprise scale

[TechRadar](#)

21%

of enterprises have mature governance in place to manage the risks of agentic AI

[Deloitte](#)

Key Capabilities

Agent Registry

- Agent discovery across client agent environments
- Inventory of built and SaaS agents

Identity Issuance

- Issues SPIFFE identities (SVIDs) in the form of X.509 certificates to AI agents
- Integrates with enterprise PKI, including DigiCert Private CA
- Uses short-lived credentials that are automatically rotated
- Supports platform attestation before issuing certificates
- Enables mTLS authentication between agents and systems
- Eliminates shared API keys and long-lived static credentials

Agent Passport

- Binds tamper-evident cryptographic trust artifact to agent identity
- Allows for fine-grained custom policy creation
- Encodes approved systems and MCP connections
- Encodes permitted operations
- Defines authorized environments of operation
- Associates approved data sensitivity classifications such as PII or PHI
- Embeds a named accountable owner responsible for the agent
- Issues and signs within a defined enterprise trust domain

Authorization

- Deploys a Policy Enforcement Point (sidecar) proxy to intercept agent traffic
- Provides MCP gateway for policy enforcement for SaaS agents
- Establishes secure encrypted communication channel using mTLS, following mutual authentication with short-lived certificates
- Evaluates passport and permits or denies actions based on evaluation
- Supports time-limited authorization via expiration and renewal controls
- Allows environmental restrictions such as development versus production
- Enables scope restriction to specific systems or APIs
- Allows temporary or purpose-specific authorization
- Supports revocation when trust conditions change

Governance

- Derives lineage from runtime enforcement and audit events
- Builds relationship graphs connecting agents to systems, models, connections, and data classifications
- Supports enforcement of additional controls such as data masking or access segregation

Lifecycle Management

- Passport issuance
- Renewal and expiration workflows
- Revocation of Passport authorization
- Auditable lifecycle state

Get started today
DigiCert invites you to join the [AI Agent Trust preview](#).

About DigiCert

DigiCert is a global leader in intelligent trust. We protect the digital world by ensuring the security, privacy, and authenticity of every interaction. Our AI-powered DigiCert ONE platform unifies PKI, DNS, and certificate lifecycle management to secure infrastructure, software, devices, messages, and AI content, agents, and models. Learn why more than 125,000 organizations, including 90% of the Fortune 500, choose DigiCert to stop today's threats and prepare for a quantum-safe future at www.digicert.com