

SOLUTION BRIEF

Cryptographic Trust for Agentic AI

Discover, identify, and monitor AI agents with Entrust Cryptographic Security Platform



ENTRUST

SECURING A WORLD IN MOTION

THE MARKET SHIFT

AI Is Moving From Assistance to Action

Organizations are rapidly moving from AI assistants that retrieve and summarize information to AI agents capable of invoking tools, calling APIs, modifying records, and taking autonomous action. As these agents gain access to enterprise systems and data, organizations face a new challenge: how to establish trust in human-like actors operating at machine speed.

AI agents are becoming a new class of enterprise identity

AI agents are not people, but they often act on behalf of people. They are not traditional machines either, because they can carry delegated authority, dynamic permissions, and increasing autonomy. The security question therefore expands from protecting what AI can access to proving which agent is acting, what authority it carries, and whether its actions can be trusted.

WHAT MAKES AN AI AGENT LOOK LIKE A MACHINE	WHAT MAKES AN AI AGENT LOOK LIKE A HUMAN
• There’s no person behind it • Accountability is delegated • It cannot authenticate using biometrics like a human • It scales beyond human limits	• Non-deterministic behavior • Dynamic permissions • Ephemeral and self-spawning • Carries human context

THE CHALLENGE

The Immediate Problem Is Still Data Protection

Most organizations do not begin with fully autonomous agents. They begin with employees and teams creating internal AI experiences under human oversight. The most immediate security need remains to protect sensitive data at rest, in motion, and in use, secure the keys that protect that data, and control where sensitive information can go.

01	02	03
Protect sensitive data	Secure cryptographic assets	Improve control and evidence
Apply encryption and key protection to the information AI applications retrieve, process, and create.	Protect encryption and signing keys and reduce exposure from unmanaged keys and secrets.	Understand where cryptography is used, apply policy, and support compliance reporting.

Agentic AI Growing in Autonomy Will Amplify Existing PKI Pressure

As AI agents become more autonomous, they call APIs, write records, use tools, delegate to other agents, and operate with less direct human oversight. Organizations therefore need a reliable way to identify each agent, connect it to accountable ownership, authenticate it across services, and manage its credentials at machine speed. The strongest way to do this is through cryptographic identity, with every agent carrying a digital certificate that proves who it is.

That creates a new challenge for PKI teams. PKI and data security teams already manage certificate sprawl, manual issuance, limited visibility, fragmented infrastructure, shorter certificate lifetimes, and growing compliance demands. Agentic AI multiplies those pressures, as potentially thousands of short-lived agents require certificates of their own, driving a sharp increase in identities, automation, and M2M and A2A communication.

WHERE PKI ALREADY STRAINS	WHAT AGENTIC AI MULTIPLIES
• Manual certificate processes and inconsistent governance • Limited visibility • Certificate sprawl • ADCS modernization • Certificate lifecycle overhead	• More machine identities • Shorter-lived identities • Higher volume and speed • More automated credential requests • More agent and service connections



THE SOLUTION

A PKI Modernization Journey, Extended to AI

Agentic identities need the same certificate lifecycle discipline as other machine identities but at higher volume and with shorter lifetimes. This is not a separate security program. It is the existing cryptographic foundation applied to a new class of identity.

The questions you typically ask about keys, certificates, and secrets now apply to your AI agents as well:

Where are AI agents deployed?	How do I identify them?	How do I secure their identities?	How do I assess compliance?
-------------------------------	-------------------------	-----------------------------------	-----------------------------

Extend cryptographic security from data to agents

The Entrust Cryptographic Security Platform helps data security, PKI, and security teams extend existing cryptographic practices to agentic AI. The platform supports practical progression: protect data and keys, discover agent ecosystems, establish cryptographic identities for AI workloads, and evaluate governance readiness. Organizations can build on PKI, certificate lifecycle automation, HSM-anchored trust, and cryptographic policy practices they already operate.

1	Discover AI agents and dependencies Start with visibility into agents, models, MCP servers, connected tools, and shared dependencies. Identify orphaned resources and understand how one dependency can affect multiple agents.
2	Establish cryptographic identities for AI agents Use certificate-based identities and automated lifecycles for AI workloads. Give services and IAM systems a verifiable identity rather than relying only on asserted names, reusable API keys, or long-lived secrets.
3	Assess AI agent compliance and governance readiness Evaluate ownership, access and data exposure, oversight and policy coverage, audit evidence, and runtime integrity alongside traditional cryptographic assets.

HOW IT WORKS

Discover AI Agents and Dependencies

You cannot secure or govern AI agents without first understanding what exists and how it connects. Entrust CSP collects inventory data to provide visibility into agents, models, MCP servers, tools, and their relationships. This helps teams identify shared dependencies, understand the systems and resources agents can reach, and uncover assets without clear ownership, creating the foundation for identity management, risk assessment, and compliance.

See the ecosystem and the relationships behind it:

- **Agents:** See what is deployed and where ownership is recorded
- **Models:** Identify model dependencies shared across agents
- **MCP servers:** Understand the connectors that give agents access to systems
- **Tools:** See what agents can invoke and where reach expands

These relationships matter. A shared model or MCP server can connect many agents to the same dependency or system. Relationship visibility helps teams move beyond a simple inventory to understand concentration, access paths, and resources without a clear owner.



Establish Cryptographic Identities for AI Agents

Entrust CSP supports certificate provisioning through SPIFFE and SPIRE. SPIFFE defines a standard identity for a workload and the credential that proves it. SPIRE attests the machine and workload, then issues and rotates a short-lived identity credential. Entrust PKI can issue the signing CA, while an HSM protects the enterprise root of trust.

01	02	03	04
AI agent	SPIRE agent	SPIRE server	Enterprise PKI and HSM
Requests an identity without carrying a static key or secret.	Attests the machine and workload.	Issues and rotates a short-lived X.509 identity credential.	Anchor the chain in a root the organization governs and audits.

Agentic AI demands an identity model that can operate at machine speed and scale. SPIFFE and SPIRE provide that model by replacing static secrets with attested workload identities, automatically rotating short-lived credentials, and applying a consistent identity framework across cloud and on-premises environments. Because every identity ultimately chains back to enterprise PKI and HSM infrastructure, organizations can extend cryptographic trust to AI agents while maintaining the governance, control, and auditability they already rely on.

Assess AI Agent Compliance and Governance Readiness

Entrust CSP Compliance Manager can evaluate AI assets across four areas:

- **Identity and ownership:** Who is this agent, where is it, and who is accountable?
- **Access and data exposure:** What can this agent access or change?
- **Oversight and policy coverage:** Is there a policy or human control for sensitive operations?
- **Audit and integrity:** Can teams prove what happened and trust the runtime?

BUSINESS OUTCOMES

Prepare for AI Autonomy Without Starting Over

The cryptographic capabilities protecting data today can become the identity and governance foundation for more autonomous AI tomorrow. Modernization reduces immediate operational pressure while creating a practical path to higher volume, shorter-lived agent identities.

Protect data now	Secure sensitive information and the cryptographic keys AI applications depend on
Improve visibility	Discover agents, dependencies, and resources without clear ownership
Reduce credential risk	Replace reusable secrets with verifiable, short-lived workload identities
Support governance	Assess ownership, access, policy coverage, audit evidence, and integrity
Build on existing investments	Extend PKI, certificate automation, and HSM anchored trust to agentic AI

Build Cryptographic Trust for Agentic AI

Protect the data AI uses today, then extend the same trusted foundation to discover, identify, and monitor AI agents as autonomy grows.

[Learn More about Entrust CSP](#)
[Talk to our Team](#)

ABOUT ENTRUST

Entrust fights fraud and cyber threats with identity-centric security that protects people, devices, and data. Our comprehensive solutions help organizations secure every step of the identity lifecycle, from verifying identity at onboarding to securing connections and fighting fraud in everyday transactions. Ongoing monitoring supports compliance and safeguards keys, secrets, and certificates. With a foundation of identity-centric security, our customers can transact and grow with confidence. Entrust has a global partner network and supports customers in over 150 countries.

For more information, visit www.entrust.com.