SOLUTION BRIEF

Securing Enterprise AI With a Hardware Root of Trust

Building a cryptographic trust layer for AI applications, agents, workloads, data, and enterprise services



ENTRUST

SECURING A WORLD IN MOTION

Contents

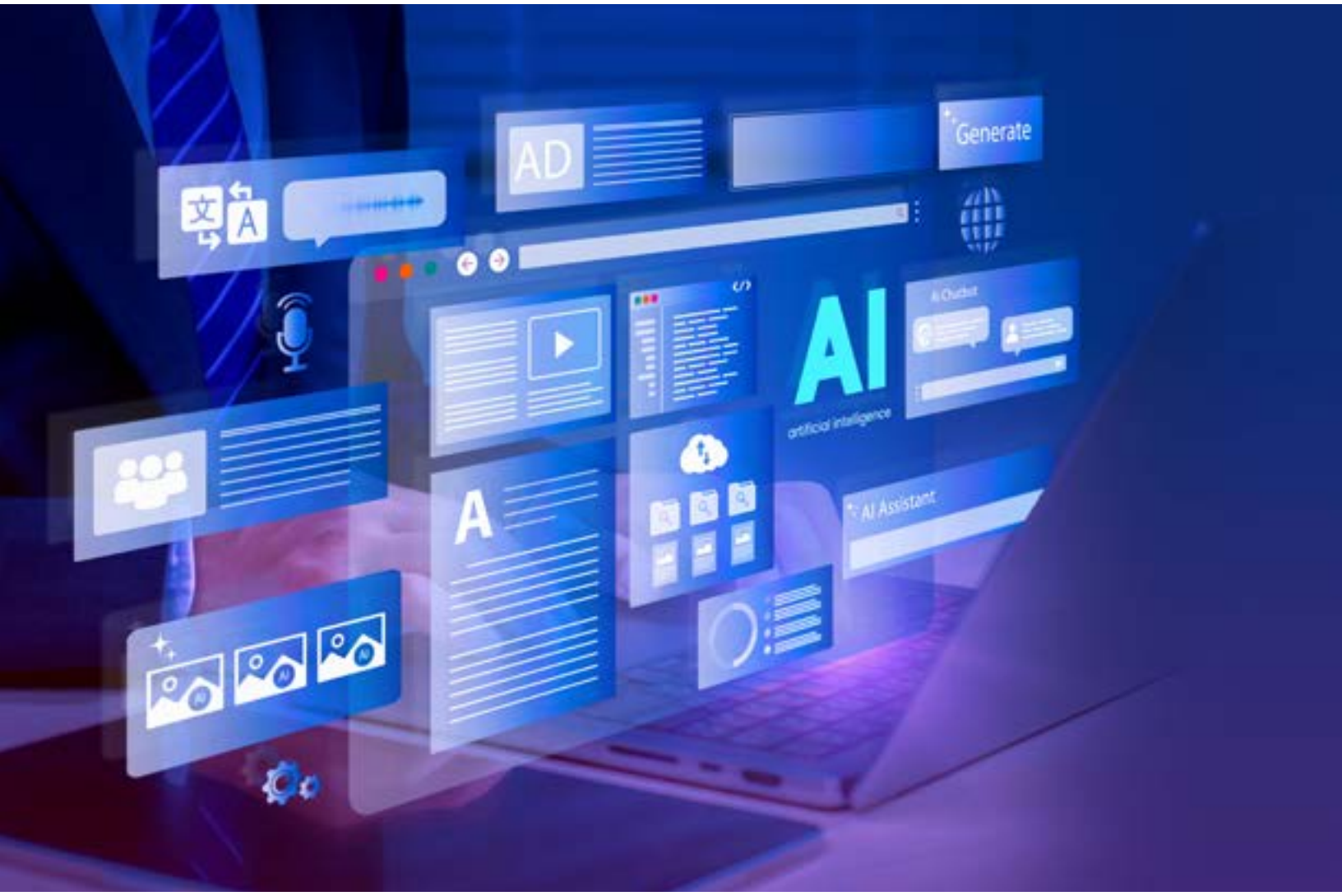
01. Building Trusted AI Infrastructure for the Enterprise 3

02. A Trust Architecture for Enterprise AI Infrastructure 5

03. Apply Cryptographic Trust Across the Enterprise AI Lifecycle 6

04. Support Enterprise AI Deployment Patterns 7

05. Build an Enterprise Trust Layer That Can Scale With AI 8



Building Trusted AI Infrastructure for the Enterprise

Enterprise AI is becoming infrastructure – not a single application. Organizations are connecting models and agents to enterprise data, APIs, business applications, orchestration services, and hybrid-cloud compute. As adoption moves from experiments to production, the security challenge expands beyond protecting a model: Enterprises need consistent identity, cryptographic protection, policy, and evidence across the infrastructure that AI depends on.

Secure the Enterprise AI Stack, Not Just the Agent

AI assistants, retrieval-augmented generation (RAG), inference services, autonomous agents, and AI-enabled applications create different workloads but rely on common trust services. Keys protect data and transactions. Certificates establish machine and workload identity. Secrets connect services. Signing establishes integrity and authenticity. Hardware security modules (HSMs) provide a hardware-backed root for critical cryptographic operations. Governance should span these assets as AI scales across teams and environments.

The Entrust Cryptographic Security Platform brings PKI, HSMs, and key, certificate, and secrets lifecycle management into a common cryptographic trust layer. nShield 5 HSMs provide hardware-backed cryptographic services, while CodeSafe can extend the HSM boundary to selected security-sensitive application logic.

What enterprises need to establish

- Identity for agents, machines, workloads, services, and APIs
- Protection for models, prompts, RAG data, inference data, credentials, and business records
- Controlled access to encryption and signing keys separated from AI application runtimes
- Scalable discovery, governance, renewal, and rotation of keys, certificates, and secrets
- Evidence connecting sensitive AI-driven actions to approved identity and cryptographic controls



A Trust Architecture for Enterprise AI Infrastructure

Enterprise AI spans several technology domains. Separating them into layers prevents trust decisions from being concentrated in the model runtime and creates reusable security control points across many AI use cases.

Enterprise Layer	Representative Components	Trust Requirement
AI Experiences & Agents	Copilots, assistants, agents, AI-enabled apps	Authenticate actors; constrain delegated authority; verify sensitive actions.
AI Platform & Orchestration	Inference endpoints, model gateways, RAG, orchestration, API/tool connectors	Protect service identity, credentials, data flows, and policy enforcement.
Data & Model Layer	Enterprise data, RAG/vector stores, model artifacts, prompts, inference data	Encrypt sensitive assets; govern keys; preserve integrity.
Compute & Cryptographic Trust	Cloud/hybrid compute, containers, HSMs, trusted security logic	Separate cryptographic authority from workloads; protect key use and sensitive logic.
Enterprise Governance	PKI, certificates, keys, secrets, inventory, lifecycle policy, audit	Operate trust services at machine speed with consistent visibility and control.

Hardware root of trust as shared enterprise infrastructure

nShield 5 HSMs anchor high-value cryptographic functions including key generation, encryption, and digital signing in tamper-resistant hardware. Instead of giving each AI application independent control of sensitive keys, enterprises can expose governed HSM-backed services to PKI, signing, encryption, and other high-assurance workflows. The nShield Security World architecture supports scalable HSM estates; nShield 5s can also support multiple tenants with separate Security Worlds and cryptographic separation.

CodeSafe when the decision itself needs protection

CodeSafe is a protected environment for selected security-sensitive code, not an AI model runtime. CodeSafe applications can execute inside the nShield boundary, be digitally signed and verified for integrity at runtime, and be associated with designated keys and certificates. In enterprise AI designs, this supports narrowly scoped policy, authorization, verification, or conditional-signing logic where the cryptographic control point should remain protected even if surrounding host software is compromised.

Apply Cryptographic Trust Across the Enterprise AI Lifecycle

Protect data and AI assets

Many enterprise deployments begin with internal assistants, RAG, and application integration. The immediate requirement is to protect sensitive information and the keys and credentials that secure it. Encryption keys should be governed independently from the AI applications consuming protected data.

- Protect enterprise and customer data retrieved by AI applications.
- Protect model artifacts, prompts, RAG stores, and inference inputs and outputs according to data sensitivity.
- Reduce exposure from unmanaged keys and application secrets through governed lifecycle controls.

Establish workload and agent identity

As AI gains autonomy, agents join an existing population of machines, workloads, APIs, and services requiring credentials and lifecycle management. Cryptographic identity allows enterprise services to authenticate the requesting workload or agent; ownership and policy determine what that identity is authorized to do.

Control sensitive AI-driven actions

For actions with material business impact, enterprises can combine identity, authorization policy, and HSM-protected signing. CodeSafe can protect deterministic decision logic governing access to designated signing keys. The business application should retain relevant context, such as the requesting identity, delegated authority, target operation, and transaction metadata, alongside cryptographic records.

Operate trust at machine speed

AI adoption increases the number of non-human identities and cryptographic assets security teams must manage. The Entrust Cryptographic Security Platform provides centralized cryptographic control, discovery, lifecycle automation, policy enforcement, and governance across keys, certificates, secrets, machines, workloads, and emerging AI agents. This enterprise control plane helps maintain consistent ownership and lifecycle policy even as AI workloads become more dynamic.



Support Enterprise AI Deployment Patterns

Enterprise copilots and RAG

Protect data sources, credentials, retrieval services, and encryption keys supporting internal AI experiences. Central key and certificate governance helps avoid creating a separate cryptographic island for every AI project.

Agentic workflows across business systems

Agents can invoke APIs, use tools, update records, and coordinate across applications. Treat agents as governed enterprise identities: Authenticate them to services, constrain authority through policy, manage credentials through their lifecycle, and use signing where downstream systems require stronger proof of sensitive actions.

AI platforms and shared model services

Central inference platforms and model gateways can serve multiple applications and business units. HSM-backed key services separate encryption, signing, and PKI authority from those runtimes. Where shared HSM infrastructure is appropriate, nShield 5s multi-tenancy can maintain independent roots of trust with separate Security Worlds and strong cryptographic separation.

Hybrid-cloud, regulated, and sovereignty-sensitive environments

The Entrust Cryptographic Security Platform supports on-premises or cloud-delivered deployment. Enterprises can align cryptographic control, key custody, and administrative boundaries with application architecture and regulatory requirements rather than tying the trust model to a single AI or cloud platform.

High-assurance approval and policy services

CodeSafe can protect sensitive business logic such as risk checks, limits, approval workflows, and conditional signing inside an nShield HSM. For AI infrastructure, use this pattern selectively for deterministic security gates around high-impact operations, while leaving probabilistic model reasoning in the AI platform.

Post-quantum and algorithm transition

AI infrastructure may outlive individual models and cryptographic algorithms. The Entrust Cryptographic Security Platform supports cryptographic inventory, CBOM, policy control, and post-quantum readiness. Current nShield 5 platforms support NIST-standardized post-quantum algorithms, while CodeSafe can support emerging or non-standard cryptographic implementations inside the HSM boundary.



Build an Enterprise Trust Layer That Can Scale With AI

The enterprise objective is not to secure one model or one agent in isolation. It is to make trusted identity, protected cryptographic authority, lifecycle management, and evidence available as shared infrastructure wherever AI touches business data, applications, APIs, and workflows.

A practical control model

1. Discover and govern cryptographic assets

Gain visibility into keys, certificates, secrets, machines, and workloads; establish policy and ownership.

2. Protect critical keys in hardware

Use nShield HSMs to anchor high-value encryption, signing, and PKI keys outside application runtimes.

3. Establish cryptographic identity

Issue and manage credentials for workloads, services, and AI agents so enterprise systems can authenticate non-human actors.

4. Protect trust-critical logic selectively

Use CodeSafe for deterministic application logic that warrants execution within the HSM security boundary and tightly controlled key access.

5. Create verifiable evidence

Use cryptographic signatures and governance records to strengthen accountability for sensitive AI-enabled actions.

6. Engineer for crypto-agility

Maintain inventory and policy so algorithms, keys, certificates, and cryptographic services can evolve without redesigning every AI application.

Entrust components in the architecture

Entrust Cryptographic Security Platform

Unified cryptographic trust layer bringing together PKI, HSMs, key, certificate, and secrets lifecycle management, discovery, governance, automation, crypto-agility, and post-quantum readiness.

Entrust nShield 5 HSMs

Hardware-backed cryptographic services for key generation and protection, encryption, signing, and enterprise roots of trust.

Entrust CodeSafe

Protected execution for security-sensitive application logic, with signed-code integrity verification, application-to-key association, policy enforcement, and support for custom or emerging cryptographic implementations.

Explore AI Security Solutions From Entrust

Move from project-by-project AI security controls to reusable enterprise trust infrastructure that supports AI applications today and increasingly autonomous agents over time.

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.

©2026 Entrust Corporation. All rights reserved. Entrust, Datacard, and the hexagon logo are trademarks, registered trademarks, and/or service marks of Entrust Corporation in the U.S. and/or other countries. All other brand or product names are the property of their respective owners. DS27Q3-securing-ai-with-hardware-root-of-trust-sb

entrust.com Toll-Free: 888.690.2424 | International: +1.952.933.1223 | sales@entrust.com

ENTRUST
SECURING A WORLD IN MOTION