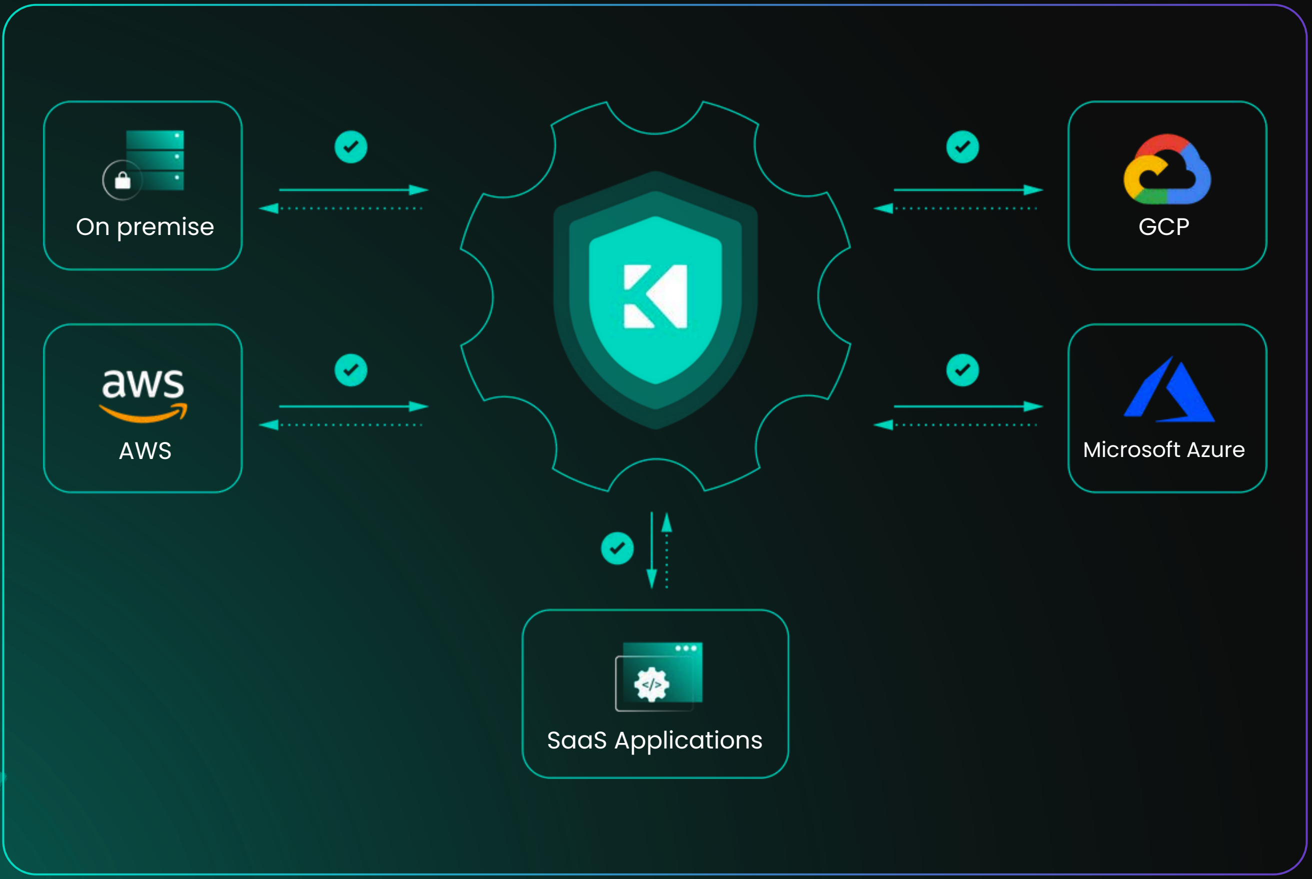
AKEYLESS

Akeyless NHI Federation

SSO for Machines

Authenticate and authorize machine identities across cloud and hybrid environments



AKEYLESS © 2025

The Challenge:
Secrets Sprawl and Security Silos

As enterprises scale across cloud, hybrid, and on-prem environments, managing machine identities becomes increasingly complex. Legacy approaches rely on static secrets, duplicated configurations, and environment-specific hacks, creating inconsistent access controls and increasing breach risk.

The Solution:
NHI Federation by Akeyless

Akeyless NHI Federation replaces static secrets with federated identity authentication for all workloads, from Kubernetes to serverless, using native cloud IAM and open standards.

- ✓ **Secretless by Design:** No stored credentials; ephemeral access tokens only
- ✓ **Zero Trust JIT Access:** All interactions authenticated & authorized in real time
- ✓ **Cross-Cloud and Hybrid Ready:** AWS, Azure, GCP and on-prem
- ✓ **Standards-Based:** Built-in support for SPIFFE/SPIRE and major cloud federation protocols

What Is NHI Federation?

Non-Human Identity (NHI) Federation is the secure authentication and authorization of machine identities, including workloads, containers, services, and scripts, across hybrid and multi-cloud environments. It replaces static secrets with federated identity protocols and cloud-native authentication.

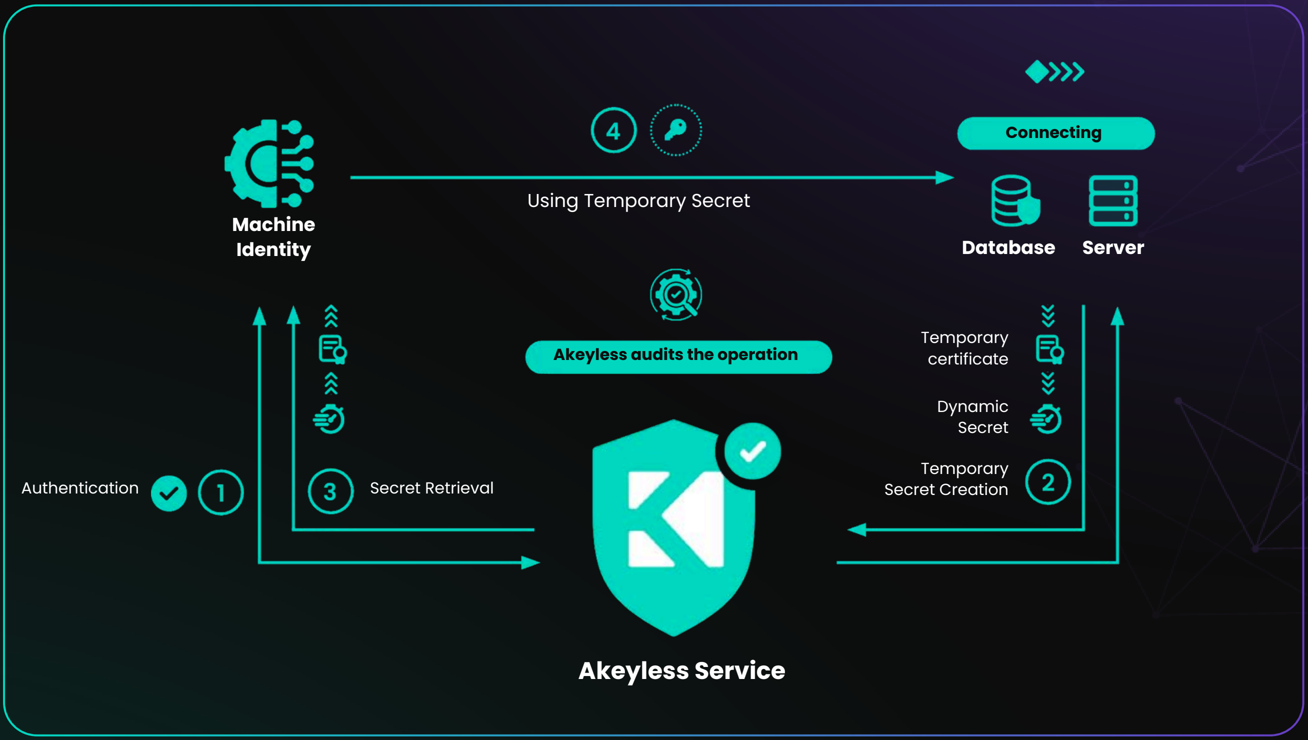
The Meaning of Single Sign-On for Machines

Single Sign-On (SSO) allows human users to access multiple systems with one secure identity.

Akeyless applies the same principle to machines: letting workloads authenticate once using their cloud identity, then securely access any approved system, without needing stored credentials.

How It Works

Federated Authentication & Temporary Access in 4 Steps



1. **Authentication**
   The machine (for example, a workload, AI agent, app or container) authenticates using its cloud-native identity (such as AWS IAM role, Azure Entra workload ID, or GCP Workload Identity).
   No static secrets are used or stored.

2. **Temporary Secret Creation**
   Akeyless issues a purpose-specific, short-lived secret, such as a dynamic DB password or X.509 certificate.

3. **Secret Retrieval**
   The machine securely retrieves the credential, with full access control and audit logging enforced.

4. **Use of Secret**
   The credential is used to access a target system (such as a database or service).

The Bottom Line: Ephemeral, identity-bound secrets enable **secure, auditable SSO for machines**.

Benefits of NHI Federation

- **Dramatically Reduce Risk**

  Eliminate one of the most common breach vectors by going fully secretless.
- **Streamline Compliance**

  Enforce consistent policies with full audit trails — across all environments.
- **Gain Operational Efficiency**

  Simplify onboarding and scaling with native integrations and centralized management.

Why Akeyless

- **Truly Secretless Architecture.** No static secrets. Ever.
- **Unified Platform.** Manage secrets, access, and identity federation in one solution.
- **Cloud-Native, Standards-Aligned.** Built for modern environments and DevOps workflows.
- **Zero-Knowledge Design.** Akeyless cannot access your credentials, by design.

Ready to Eliminate Machine Credentials?

REQUEST A DEMO TODAY

or visit us at akeyless.io

AKEYLESS © 2025