AKEYLESS

Major European Financial Institution Strengthens Identity Security and Resilience for the AI Era

Background

A major European financial institution with extensive global footprint operates a complex hybrid environment spanning on-premise infrastructure, cloud services, and globally distributed operations. As the organization expanded its digital services and automation initiatives, security teams needed a scalable approach to managing secrets, privileged access, cryptographic controls, and operational resilience while meeting stringent regulatory requirements.

At the same time, the Institution was beginning to evaluate emerging AI use cases, creating new requirements for secure, policy-driven access to sensitive systems and data. The organization sought a unified approach that could strengthen security today while supporting future innovation.

Industry

Financial Services

Region

Europe, with global technology and operations teams

Environment

Hybrid multi-cloud and on-premises infrastructure

Results at a Glance

- Multi-region resilience and disaster recovery readiness
- Customer-controlled cryptographic protection with DFC™ and HSM-backed key management
- Governance for code signing, certificates, key replication, and secrets management
- Secure foundation for AI and automation initiatives with zero-credential agent access and intent-based authorization

The Challenge

As the organization expanded its digital services and automation initiatives, it faced a growing set of security, resilience, and governance requirements across a complex global technology environment.

- **Centralizing secrets and privileged access:** The Institution needed to operationalize secrets management across hybrid infrastructure while supporting static and dynamic

credentials, shared targets, self-service workflows, CRM integrations, and cloud-native access patterns. In parallel, teams were modernizing password management and privileged access workflows.

- **Strengthening resilience and regional availability:** To support global operations, the organization required additional regional SaaS support in APAC, along with disaster recovery and point-in-time recovery (PITR) readiness, secure network controls, and customer-managed gateway deployments.
- **Scaling cryptographic operations and governance:** Security teams needed to support code-signing workflows, certificate management, KMS key replication across regions, HSM-backed key protection, and long-term key rotation requirements driven by internal security and regulatory policies.
- **Preparing for emerging AI access patterns:** As the Institution explored AI initiatives, it sought a way to extend its zero-trust approach to AI agents and automated systems while maintaining policy enforcement, auditability, and control over access to sensitive resources.

The Solution

The Institution recognized that addressing each challenge independently would increase operational complexity and create additional security silos. Instead, it sought a unified platform that could support secrets management, privileged access, cryptographic operations, resilience requirements, and emerging AI initiatives through a consistent security and governance model.

After evaluating its requirements, the organization selected Akeyless to provide a centralized, highly secured approach to identity security across its hybrid environment. The platform's cloud-native architecture, multi-region deployment capabilities, and broad integration ecosystem aligned with the Institution's operational and resilience requirements. Akeyless patented Distributed Fragments Cryptography™ (DFC) and zero-knowledge security model enabled customer-controlled cryptographic protection, supporting the organization's security and regulatory objectives.

Over time, Akeyless has expanded to support multiple strategic initiatives across the organization, helping security and infrastructure teams standardize how secrets, access, cryptographic assets, and operational controls were managed across cloud and on-premise environments.

Key Initiatives Supported

- Enterprise secrets management for applications and internal platforms
- Dynamic and static secrets workflows for operational tooling
- Password management modernization and end-user rollout
- CRM integration for secrets-related workflows and approvals
- Regional SaaS resilience, disaster recovery, and PITR readiness

- IP allow listing and network access controls for regulated environments
- Code-signing certificates and key management workflows
- Multi-region KMS key replication ensuring consistent cryptographic governance
- HSM-backed key fragment protection and rotation planning
- Secure AI agent access and governance for emerging AI and automation initiatives

The Results

By adopting a unified platform approach, the Institution was able to expand beyond its initial secrets management deployment and support a broader set of security, resilience, and governance initiatives through a consistent operating model.

Key outcomes included:

- **Expanded platform adoption across multiple security programs**, supporting secrets management, password management, cryptographic operations, resilience initiatives, and emerging AI-related security requirements.
- **Strengthened regional resilience and operational continuity** through additional regional SaaS support in additional GEOs, disaster recovery planning, and point-in-time recovery readiness to support global availability requirements.
- **Established a scalable framework for cryptographic governance**, supporting code-signing workflows, certificate management, KMS key replication across regions, and long-term key rotation requirements.
- **Maintained customer control over sensitive cryptographic material** through HSM-backed key fragment protection, helping align security controls with internal governance and regulatory requirements.
- **Standardized security controls across hybrid environments**, enabling teams to manage secrets, credentials, and operational access through a consistent platform spanning cloud and on-premise infrastructure and applications, such as ServiceNow, GitHub Actions, SafeBreach, GCP, Azure, Oracle, MS SQL, Active Directory, LDAP.
- **Enabled secure adoption of AI agents and automated systems**, eliminating credential exposure through zero-credential access, enforcing intent-based authorization through RBAC and ABAC policies, and providing full traceability of agent actions across internal systems.

Secure identity and access across financial services

Request a demo to see how at akeyless.io/demo.