AKEYLESS

Akeyless DFC™: Zero-Knowledge Secrets Management for Regulated Enterprises

Akeyless Distributed Fragments Cryptography (DFC™) removes the need for vendor trust by ensuring only you can access your secrets and keys.

The End of the SaaS Trust Dilemma

Regulated enterprises have long faced a trade-off between control and agility. On-premises vaults and hardware security modules (HSMs) provide ownership of encryption keys but create complexity, expense, and operational drag. SaaS models offer scale and simplicity but require trusting the provider with sensitive cryptographic material, unacceptable for organizations bound by strict compliance and data sovereignty mandates.

Akeyless eliminates that compromise. Its patented Distributed Fragments Cryptography (DFC™) technology delivers the efficiency of SaaS with the control of on-prem systems. The result is a new model for protecting secrets, certificates, and encryption keys that replaces trust with cryptographic proof.

Key Benefits

- True zero-knowledge key ownership
- Keys fragmented across regions and cloud providers, never combined
- Continuous fragment refresh for cryptographic resilience
- SaaS-level simplicity with on-prem-level security
- Automated rotation and just-in-time access
- Compliance-ready for regulated industries

AKEYLESS

The Technology: Distributed Fragments Cryptography (DFC™)

At the core of the Akeyless platform is DFC™, a NIST FIPS 140-2 validated cryptographic method that fragments encryption keys across multiple regions and cloud providers. Unlike conventional vault-based systems that store complete keys in one place, DFC ensures no single entity ever holds the full key.

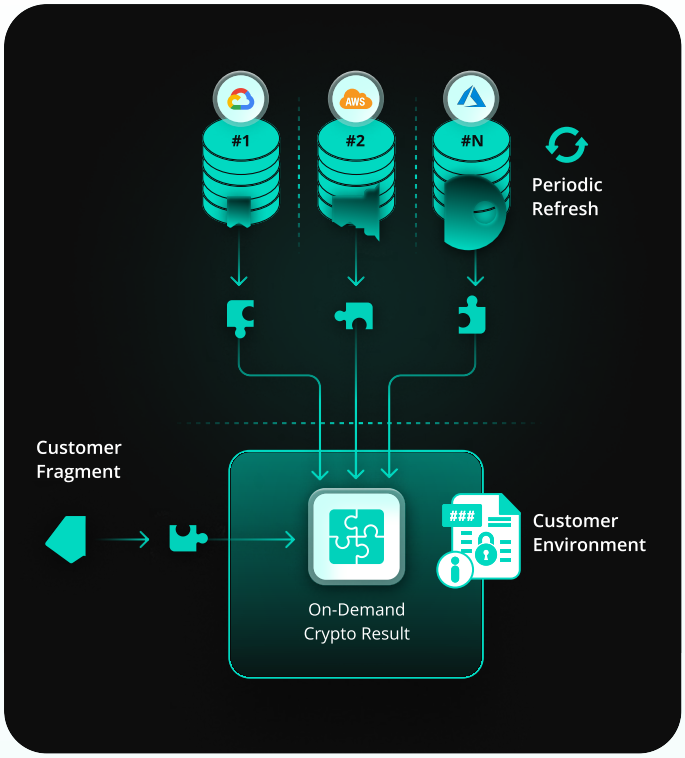
Cryptographic operations such as encryption, decryption, and signing occur without ever recombining the fragments, ensuring sensitive data remains fully protected. DFC also refreshes the mathematical values of those fragments continuously while preserving the key's integrity, preventing static vulnerabilities and insider risk. The result is HSM-grade assurance with the flexibility and automation of a cloud-native service, helping your organization strengthen protection for sensitive assets without the complexity of hardware management.

Case in Point: A Global Financial Institution

A leading global bank had long prohibited SaaS-based key management due to regulatory and risk concerns. After rigorous evaluation, the bank deployed the Akeyless Gateway within its own environment and verified through independent testing that Akeyless could not access or reconstruct its encryption keys.

The deployment passed internal and external security audits, proving that zero-knowledge SaaS can meet the highest compliance and data-sovereignty standards. The result was a secure migration to a modern, automated secrets management platform without losing sovereignty or visibility.

AKEYLESS



Zero-Knowledge by Design

DFC enables a true zero-knowledge architecture in which Akeyless has no ability to view or reconstruct your secrets, certificates, or encryption keys. One fragment always remains in your environment, managed through the Akeyless Gateway.

The Gateway is stateless, lightweight, and connects only outbound to the Akeyless SaaS service, eliminating inbound access paths. Even in a theoretical platform breach, attackers would find only incomplete, cryptographically inert fragments. Key ownership and sovereignty remain fully with your organization by design, not by policy.

Security and Compliance for Regulated Enterprises

Akeyless DFC™ gives your security and compliance teams the confidence to modernize without compromise.

Built for the Most Demanding Environments

Full key ownership: Customers retain exclusive control over one DFC fragment, guaranteeing independence from the vendor.

Simplified operations: No vault replication or hardware lifecycle management, reducing cost and complexity.

Dynamic protection: Constant key fragment refresh protects against evolving threats.

Regulatory readiness: Certified and aligned with FIPS 140-2, SOC 2 Type II, ISO 27001, and GDPR requirements.

Cloud scalability: Securely supports multi-cloud and hybrid environments while maintaining compliance boundaries.

Control Without Compromise

Akeyless DFC™ technology redefines secrets management for enterprises that need both security and agility. By engineering trust out of the equation, it delivers a zero-knowledge SaaS model that meets the strictest compliance and data-sovereignty standards.

Akeyless delivers the scale of SaaS with the assurance of cryptographic separation, ensuring your keys and data always remain under your control.

See DFC™ in action.

Request a demo at **akeyless.io/demo**