Secrets Management in Azure Key Vault/AWS KMS Training Course

Professional Development Training Course Outline

Category	Data Security	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

This intensive, hands-on course addresses the critical need for secure credential management in modern cloud environments, focusing on the industry-leading solutions: Azure Key Vault (AKV) and AWS Key Management Service (KMS). As DevOps and Multi-Cloud Architecture drive rapid deployment, the risk of hard-coded credentials, exposed API keys, and non-rotated encryption keys has become a primary security vulnerability. Secrets Management in Azure Key Vault/AWS KMS Training Course empowers Cloud Security Engineers and DevOps Professionals to master the lifecycle of digital secrets, moving from fragmented, high-risk storage to centralized, auditable, and automated secrets vault implementation. Participants will gain practical expertise in Hardware Security Module (HSM)-backed security, Role-Based Access Control (RBAC), and implementing Zero Trust principles across diverse cloud workloads.

The curriculum is designed to bridge the gap between theoretical cloud security best practices and real-world deployment challenges in a multi-cloud setting. By comparing and contrasting AKV and AWS KMS, learners will develop a strategic, vendor-agnostic understanding of Key Management and Secret Rotation. A heavy emphasis is placed on Infrastructure as Code (IaC) using tools like Terraform/ARM templates for provisioning and leveraging Managed Identities for applications to eliminate the need for embedding credentials. You'll learn to secure everything from database connection strings and TLS/SSL certificates to complex customer-managed keys (CMK), ensuring regulatory compliance and robust defense against the most common cloud-native threats.

Programme Curriculum

Secrets Management in Azure Key Vault/AWS KMS Training Course

Introduction

This intensive, hands-on course addresses the critical need for secure credential management in modern cloud environments, focusing on the industry-leading solutions: Azure Key Vault (AKV) and AWS Key Management Service (KMS). As DevOps and Multi-Cloud Architecture drive rapid deployment, the risk of hard-coded credentials, exposed API keys, and non-rotated encryption keys has become a primary security vulnerability. Secrets Management in Azure Key Vault/AWS KMS Training Course empowers Cloud Security Engineers and DevOps Professionals to master the lifecycle of digital secrets, moving from fragmented, high-risk storage to centralized, auditable, and automated secrets vault implementation. Participants will gain practical expertise in Hardware Security Module (HSM)-backed security, Role-Based Access Control (RBAC), and implementing Zero Trust principles across diverse cloud workloads.

The curriculum is designed to bridge the gap between theoretical cloud security best practices and real-world deployment challenges in a multi-cloud setting. By comparing and contrasting AKV and AWS KMS, learners will develop a strategic, vendor-agnostic understanding of Key Management and Secret Rotation. A heavy emphasis is placed on Infrastructure as Code (IaC) using tools like Terraform/ARM templates for provisioning and leveraging Managed Identities for applications to eliminate the need for embedding credentials. You'll learn to secure everything from database connection strings and TLS/SSL certificates to complex customer-managed keys (CMK), ensuring regulatory compliance and robust defense against the most common cloud-native threats.

Course Duration

5 days

Course Objectives

1. Design and implement robust, centralized secrets management strategies across Azure and AWS.
2. Distinguish the core capabilities, security tiers, and optimal use-cases for both services.
3. Master the creation, storage, rotation, and deletion of cryptographic keys and customer-managed keys
4. Explain and configure HSM-backed key protection for the highest security and FIPS 140-2 compliance.
5. Develop a cohesive secrets strategy for hybrid and multi-cloud environments.
6. Implement fine-grained access control using Azure RBAC and AWS IAM Policies for secrets and keys.
7. Securely integrate applications using Azure Managed Identities and AWS IAM Roles to eliminate embedded secrets.
8. Implement automatic and on-demand secret rotation for database credentials and API keys using Lambda/Azure Functions.
9. Integrate secrets management securely into CI/CD Pipelines
10. Provision and manage Key Vaults and KMS Keys using Terraform and ARM templates/CloudFormation.
11. Apply KMS/AKV for Transparent Data Encryption and securing data across services
12. Configure comprehensive logging, monitoring, and alerting for regulatory requirements.
13. Identify and mitigate common risks like secret sprawl, hardcoded secrets, and over-privileged access.

Target Audience

1. Cloud Security Engineers
2. DevOps Engineers
3. Cloud Architects
4. Security/Compliance Analysts
5. Software Developers
6. Infrastructure Engineers
7. System Administrators.

8. IT Auditors

Course Modules

Module 1: Introduction to Cloud Secrets & Key Management Fundamentals

- Defining Secrets Sprawl and the risks of hardcoded credentials.
- Comparison of AWS KMS and Azure Key Vault.
- Understanding the Cryptographic Primitives.
- The role of Hardware Security Modules and FIPS 140-2 compliance.
- Case Study: Analyzing the compromise of a database via a hardcoded connection string in a public GitHub repository.

Module 2: Azure Key Vault Implementation and Core Concepts

- Provisioning AKV via Azure Portal and Terraform/ARM Templates.
- Managing Secrets, Keys, and Certificates
- Configuring Access Policies and Azure RBAC for data plane access.
- Network Security.
- Case Study: Implementing a secure rotation for a SQL Database password using an AKV secret and Azure Function.

Module 3: AWS Key Management Service (KMS) Deep Dive

- Creating and managing Customer Master Keys and their properties
- Key Policy creation and applying Least Privilege access controls with IAM.
- Using Envelope Encryption and the AWS KMS APIs
- Integrating KMS with other AWS services for Encryption at Rest.
- Case Study: Designing a cross-account access strategy for a multi-region disaster recovery scenario using KMS key policies and IAM roles.

Module 4: Secure Application and Service Access

- Implementing Azure Managed Identities for App Service/VM access to AKV.
- Using AWS IAM Roles and EC2 Instance Profiles to grant KMS/Secrets Manager access.
- Best practices for Non-Human Identity access and secure bootstrap processes.
- Integrating secrets references directly into Azure App Configuration/AWS Parameter Store.
- Case Study: Migrating an existing application to use Managed Identities/IAM Roles, removing all plaintext configuration files.

Module 5: Secret Rotation and Lifecycle Automation

- Automating Secret Rotation in Azure using Event Grid and Azure Functions/Logic Apps.
- Implementing AWS Secrets Manager for integrated database credential rotation
- Developing custom rotation strategies using AWS Lambda for non-native secrets
- Managing Key Versioning and planning for zero-downtime key rotation.
- Case Study: Building a complete, automated rotation pipeline for a third-party API key that must be rotated every 90 days.

Module 6: DevOps & Infrastructure as Code (IaC) Integration

- Consuming secrets securely in Azure DevOps Pipelines/GitHub Actions

- Injecting secrets into Kubernetes/AKS/EKS workloads using CSI Drivers or native integrations.
- Using Terraform to provision the secrets infrastructure and manage policies.
- Securing Deployment Credentials used by CI/CD agents
- Case Study: Deploying a full three-tier application using Terraform, injecting database and API secrets into the application environment via a Kubernetes Secret backed by AKV/Secrets Manager.

Module 7: Certificates and Advanced Cryptographic Operations

- Automated provisioning and renewal of TLS/SSL Certificates in Azure Key Vault.
- Importing and using BYOK for both AKV and KMS.
- Understanding Data Keys and client-side and server-side encryption/decryption models.
- Configuring Multi-Region Keys and replication strategies.
- Case Study: Onboarding an external CA to auto-renew a public-facing website's SSL certificate via Key Vault.

Module 8: Security, Audit, and Compliance

- Configuring Azure Monitor/Log Analytics and AWS CloudTrail/CloudWatch for secrets activity.
- Detecting and responding to unauthorized access attempts and key usage anomalies.
- Reviewing security logs for Regulatory Compliance reporting.
- Implementing GuardDuty/Azure Security Center recommendations for secrets management.
- Case Study: Analyzing a simulated insider threat scenario by reviewing CloudTrail and Key Vault audit logs to determine the extent of a potential secret exfiltration.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call +254769199797

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
23 Nov 2026	27 Nov 2026	Online	$1,000
23 Nov 2026	27 Nov 2026	Physical	$1,500
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$4,500
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$6,000

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com