

Central Networks & Technologies Ltd

Keeper Secrets Manager Service Definition



Crown
Commercial
Service

Prepared by: Vicki Coleman
Date: 15/01/2026

 info@centralnetworks.co.uk

 +44 (0)1706 747474

 www.centralnetworks.co.uk



Central Networks and Technologies Ltd (Central) was founded in September 1991 by Christopher Mycock. In the earlier years Central was responsible for running the core ICT systems for many of the UK Magistrates Courts Services, which involved moving and hosting the mainframes and employing staff via TUPE. We also have a focus in the Housing Association and not-for-profit sector. In the last 10 years we have migrated many of our customers to cloud or partial cloud provision.

Our customer base is diverse in terms of size, geography, skills, business requirements and objectives. We have recognised this and created a solutions and services portfolio that can be tailored to meet the individual requirements of all our customers. Some of our customers have large ICT teams and only look for assistance where they have investigated and exhausted every avenue. Others are far smaller, where finance officers often take on ICT responsibility and need additional help and assistance. Central provides a bespoke service to each of our customers, providing best value for money and an ICT service which matches their requirements which assists them in delivering their objectives.

Keeper Secrets Manager – Service Definition

Keeper Secrets Manager (KSM) is a zero-knowledge, zero-trust secrets management platform designed to securely store, manage, and deliver sensitive credentials, API keys, certificates, tokens, and other machine identities. Unlike traditional secrets managers, KSM requires no vaulting infrastructure, offering a fully cloud-based, client-side encrypted solution suitable for modern DevOps, cloud-native, and automation-driven environments.

KSM ensures that secrets are never exposed in plaintext to Keeper, its infrastructure, or any intermediaries—everything is encrypted before leaving the device or system.

Core Features

1. Zero-Knowledge Secrets Storage

- Local AES-256 and elliptic curve encryption
- Keeper never has access to encryption keys
- Supports structured and unstructured secrets (keys, JSON, certificates, etc.)

2. Agentless & Infrastructure-Free Deployment

- No servers, vault appliances, or hardware
- APIs, SDKs, and CLI for instant integration
- Ideal for multi-cloud, containerised, and serverless environments

3. Fine-Grained Access Control

- Least-privilege access through RBAC
- Secure sharing with DevOps, developers & automation tools
- Full audit trail and versioning for all secret access actions

4. Dynamic & Programmatic Secret Retrieval

- Runtime retrieval via SDK/CLI
- Supports Go, Python, Java, Node.js, .NET and more
- CI/CD integrations (GitHub Actions, GitLab, Jenkins, Azure DevOps)

5. Rotation & Lifecycle Automation

- Integrated with Keeper Rotation
- Supports automated rotation of DB credentials, cloud IAM identities, SSH keys, and privileged accounts

6. End-to-End Audit & Compliance

- Logs all retrievals, changes, and administrative actions

- Supports ISO 27001, SOC 2, HIPAA, PCI DSS, GDPR, FedRAMP and more

Optional Service Delivery Central Networks

Onboarding & Setup

- Tenant initialisation and core policy setup
- Integration with Keeper Enterprise (SSO/SCIM/RBAC)
- Secure folder and role creation

Secrets Migration & Structuring

- Review of current storage locations
- Secure ingestion into encrypted KSM structure
- Re-organisation aligned to DevOps workflows

CI/CD & Cloud Integration

- Configuration for:
 - GitHub Actions
 - GitLab CI
 - Azure DevOps
 - Jenkins
 - Terraform
 - Kubernetes (KSM Operator)
- Application-level runtime secret injection

Ongoing Management & Governance

- Monthly access audits
- Rotation scheduling and enforcement
- Monitoring for access anomalies or misconfigurations

Benefits

- Eliminates plaintext secrets in code, pipelines, and infrastructure
- No servers to maintain — fully cloud-native
- Strong zero-trust and zero-knowledge enforcement
- Seamless DevOps integration
- Full compliance alignment for regulated sectors

Confidentiality and Copyright

This document and the information set out herein is confidential and is not to be disclosed or discussed with any person or party not associated with the selection of a service provider. The information in this proposal is a suggested technical offering. We reserve the right to amend or withdraw our proposal. Any typographical, clerical or other error or omission shall be subject to correction without any liability. The copyright in this proposal and any associated information or documents that we may provide remains vested in Central Networks and Technologies Ltd.