IBM Technology

G-Cloud 15
IBM – HashiCorp Vault

Service Definition Document

Email: ukcat@uk.ibm.com
Contact: Anne-Marie Wheeler

Contents

Overview

This Service Definition describes HashiCorp Cloud Platform (HCP) Vault, a managed cloud service that provides secure secrets management, encryption as a service, and identity based access control for applications and infrastructure.

HCP Vault enables UK public sector organisations to centrally manage sensitive data such as credentials, API keys, tokens, and certificates, supporting secure digital service delivery while meeting governance, audit, and compliance requirements.

HashiCorp Vault enables the UK Government to centrally eliminate credential-based cyber risk across all digital services by replacing static secrets, shared credentials, and manual key management with identity-based, policy-driven, and fully auditable security controls.

It provides a single, cloud-agnostic security control plane for secrets, encryption, and access to sensitive data—reducing the likelihood and impact of breaches, improving audit outcomes, and enabling secure digital delivery at national scale

1. What is the Service?

HCP Vault is HashiCorp's fully managed, enterprise-grade secrets and encryption platform delivered as a cloud service.

The service provides a secure system of record for secrets and cryptographic operations, enabling applications, platforms, and users to authenticate, retrieve secrets dynamically, and encrypt or decrypt sensitive data without embedding secrets in code or configuration files.

HCP Vault removes the operational burden of deploying, securing, scaling, and maintaining Vault infrastructure while providing enterprise controls, availability, and support.

2. Service Category (G-Cloud Alignment)

This service aligns to the following G-Cloud service categories:
Cloud Software

- Application security
- Information and communication technology (ICT)
- Software development tools
- Operations management

Cloud Support (optional associated services)

- Security services

- Set up and migration
- Ongoing support
- Training

3. How the Service Works

HCP Vault operates as a centrally managed control plane for secrets and encryption.
Key operational principles include:

- Secrets are stored securely and accessed dynamically at runtime
- Applications authenticate using trusted identity sources rather than static credentials
- Secrets are issued on-demand and can be short-lived
- Access is controlled through fine-grained policies
- All access and operations are logged for audit purposes

The service integrates with cloud platforms, identity providers, and application runtimes to support modern, distributed architectures.

4. Core Service Features

4.1 Secrets Management

HCP Vault securely stores and manages sensitive data, including:

- Database credentials
- API keys
- Tokens
- Passwords
- Certificates

Secrets can be dynamically generated and automatically rotated, reducing the risk associated with long-lived credentials.

4.2 Encryption as a Service (Data Protection)

HCP Vault provides cryptographic services that allow applications to encrypt and decrypt data without managing encryption keys directly.

Capabilities include:

- Centralised key management
- Encryption and decryption APIs
- Key rotation and lifecycle management
- Support for application-level encryption use cases

This enables sensitive data to be protected throughout its lifecycle.

4.3 Identity-Based Access Control

Access to secrets and cryptographic operations is governed by identity-based policies.
HCP Vault integrates with:

- Cloud identity platforms
- Enterprise identity providers
- Application and workload identities

This enables authentication without embedding static secrets and supports least-privilege access models.

4.4 Policy and Governance

Policies define who or what can access secrets and under what conditions.
Policies support:

- Fine-grained access control
- Segregation of duties
- Environment separation (e.g. development, test, production)
- Alignment with organisational security standards

Policies are enforced consistently across all access methods

4.5 Audit Logging and Compliance

All access to secrets and cryptographic operations is logged.

Audit logs include:

- Identity of the requester
- Time and type of operation
- Target secret or cryptographic action

These logs support security monitoring, incident investigation, and compliance reporting.

5. Why the Service Is Needed (Public Sector Context)

UK Government organisations operate complex digital services that rely on multiple systems, platforms, and third-party integrations.

Traditional approaches to secrets management—such as storing credentials in configuration files or environment variables—introduce significant security and operational risk.

HCP Vault addresses these challenges by:

- Eliminating hard-coded secrets
- Centralising control of sensitive data
- Enabling secure automation and DevSecOps practices
- Improving auditability and assurance
- Reducing the impact of credential compromise

6. Service Options

Deployment Model

- Fully managed SaaS delivered via HashiCorp Cloud Platform
- No customer-managed infrastructure required

Hosting Locations

- Available in European regions to support UK public sector data residency considerations

Integration Options

- Public cloud platforms (e.g. AWS, Azure, GCP)
- Enterprise identity providers
- Application runtimes and CI/CD pipelines

7. Onboarding and Offboarding

Onboarding

- Service provisioning through HashiCorp Cloud Platform
- Configuration of authentication methods and policies

- Optional support for initial setup and migration

Offboarding

- Controlled export or revocation of secrets
- Secure deletion of stored secrets in accordance with service term

8. Service Levels and Availability

- HCP Vault is provided with commercially backed service levels suitable for production workloads.
- Availability targets, service credits, and exclusions are defined contractually and apply to production use.

9. Backup, Restore, and Disaster Recovery

The service includes:

- Managed backup of service data
- High availability architecture
- Disaster recovery procedures operated by HashiCorp

Recovery objectives are defined in contractual documentation

10. Security

Security controls include:

- Encryption of data at rest and in transit
- Role-based and policy-driven access control
- Secure authentication mechanisms
- Continuous monitoring and logging

Customers remain responsible for configuring access policies and ensuring compliance with applicable regulations.

11. Access to Data on Exit

Customers retain ownership of their data.
Upon exit, customers can:

- Revoke access credentials
- Export relevant configuration where supported
- Ensure secrets are securely deleted in line with service processes

12. After-Sales Support

Support includes:

- Access to HashiCorp support portals
- Incident and problem management
- Service updates and maintenance handled by HashiCorp

Support is included with the service subscription.

13. Service Constraints

- The service is delivered as a standardised SaaS offering
- Customisation is limited to configuration and policy definition
- Maintenance is managed by the service provider

14.Technical Requirements

- Network connectivity to the HashiCorp Cloud Platform
- Supported authentication integrations
- Compatible application or platform integrations

15. Conclusion

HCP Vault provides UK Government organisations with a secure, scalable, and enterprise ready service for secrets management and encryption.

By centralising control of sensitive data and embedding security into application and infrastructure workflows, the service supports modern digital delivery while meeting public sector security and assurance requirements