DATA TEKNOLOGI SEMESTA

Vault

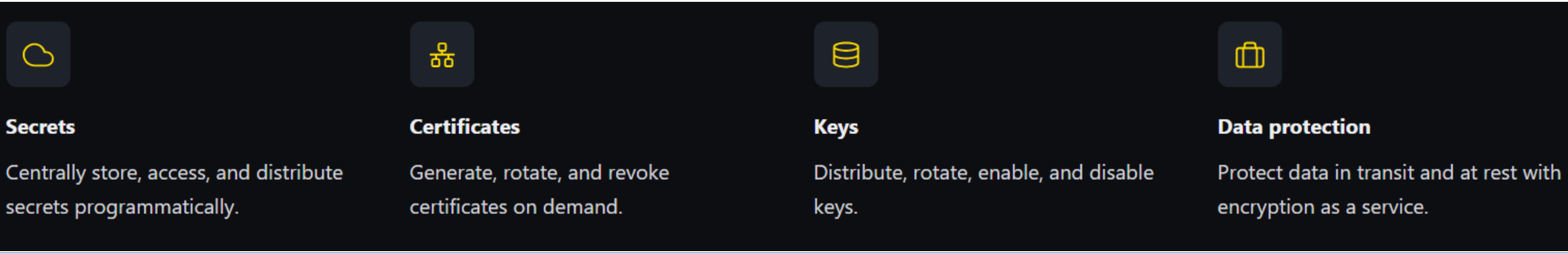
SECURITY LIFECYCLE MANAGEMENT

DATA TEKNOLOGI SEMESTA

Vault | INTRODUCTION

Vault by HashiCorp is a software tool designed to securely store and manage sensitive data such as secrets, passwords, API keys, and certificates. It acts as a centralized vault for protecting this information and ensures that access is controlled, logged, and auditable.

Vault provides organizations with identity-based security to automatically authenticate and authorize access to secrets and other sensitive data.



Vault | INTRODUCTION

DATA TEKNOLOGI SEMESTA

Vault by HashiCorp is a software tool designed to securely store and manage sensitive data such as secrets, passwords, API keys, and certificates. It acts as a centralized vault for protecting this information and ensures that access is controlled, logged, and auditable.

Vault provides key features such as:

- **Secret Management**: Allows storing and retrieving secrets dynamically, reducing hardcoded credentials in applications.
- **Encryption-as-a-Service**: Provides APIs to encrypt and decrypt data without exposing encryption keys to the end user.
- **Access Control**: Integrates with identity systems to grant or deny access to secrets based on defined policies.
- **Dynamic Secrets**: Generates credentials on demand, such as database passwords or cloud API keys, which automatically expire after a specified period.
- **Auditing and Logging**: Tracks all actions and access attempts, providing transparency and enhancing security.

Vault

Automate secure access and lifecycle management for credentials and sensitive data

DATA TEKNOLOGI SEMESTA

Identity-based security

Secrets	Certificates	Keys	Data Protection
Static	PKI	KMS	Encryption
Rotated	Managed Keys	KMIP	Signatures
Dynamic		HSM	Tokenization
Database			

Vault

Secure your credentials on day one and beyond

DATA TEKNOLOGI SEMESTA

Protect

Store secrets, certificates, and keys securely

Reduce risk with secret rotation, dynamic secrets, and just-in-time credentials

Automate tokenization and encryption of sensitive data

Inspect

Scan code repositories to identify unmanaged and exposed secrets

Prioritize action based on risk profile and activity

Identify if secret is stored and needs to be rotated

Connect

Authenticate and authorize every access request with identity

Integrate with your preferred identity access management (IAM) provider

Limit machine and database access based on policy and role

Vault

Secure your credentials on day one and beyond

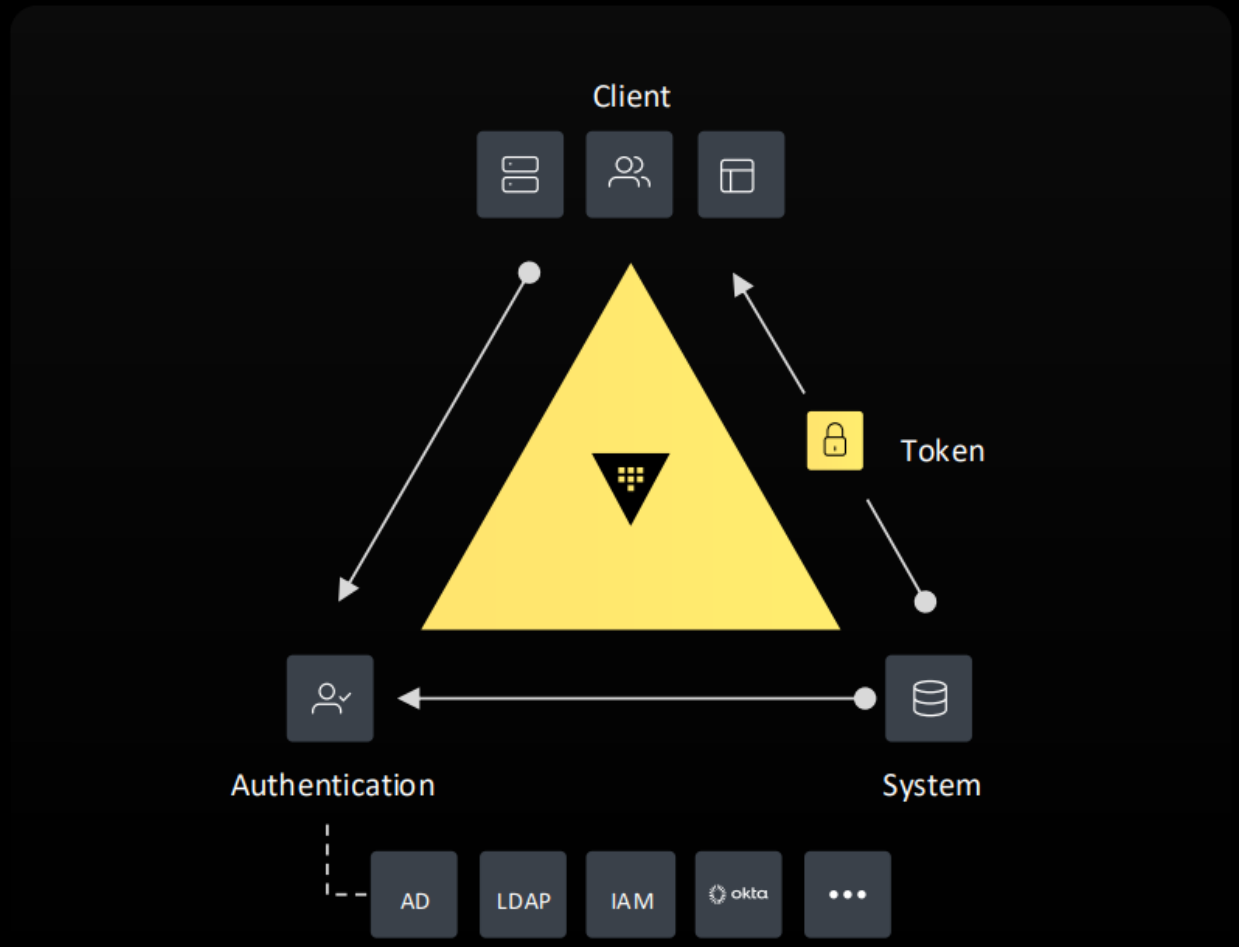
DATA TEKNOLOGI SEMESTA

In dynamic cloud infrastructure, security starts with identity.

Identity-based security uses trusted identities to automate access to secrets, data, and applications

Security system of record to centrally store and protect secrets across clouds and applications

Lifecycle management of your credentials to ensure proper oversight, rotation, and expiry

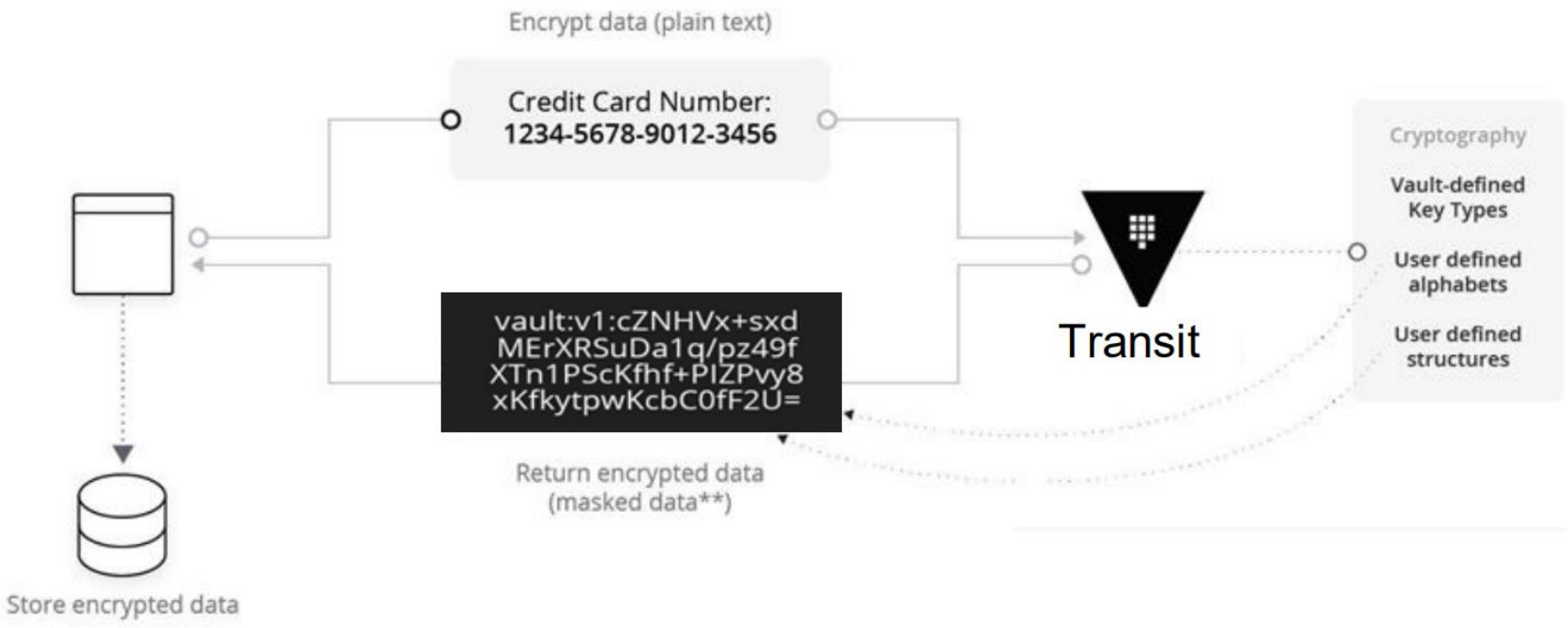


Vault | How Vault Works

DATA TEKNOLOGI SEMESTA

Data Encrypted

Transit Secrets Engine

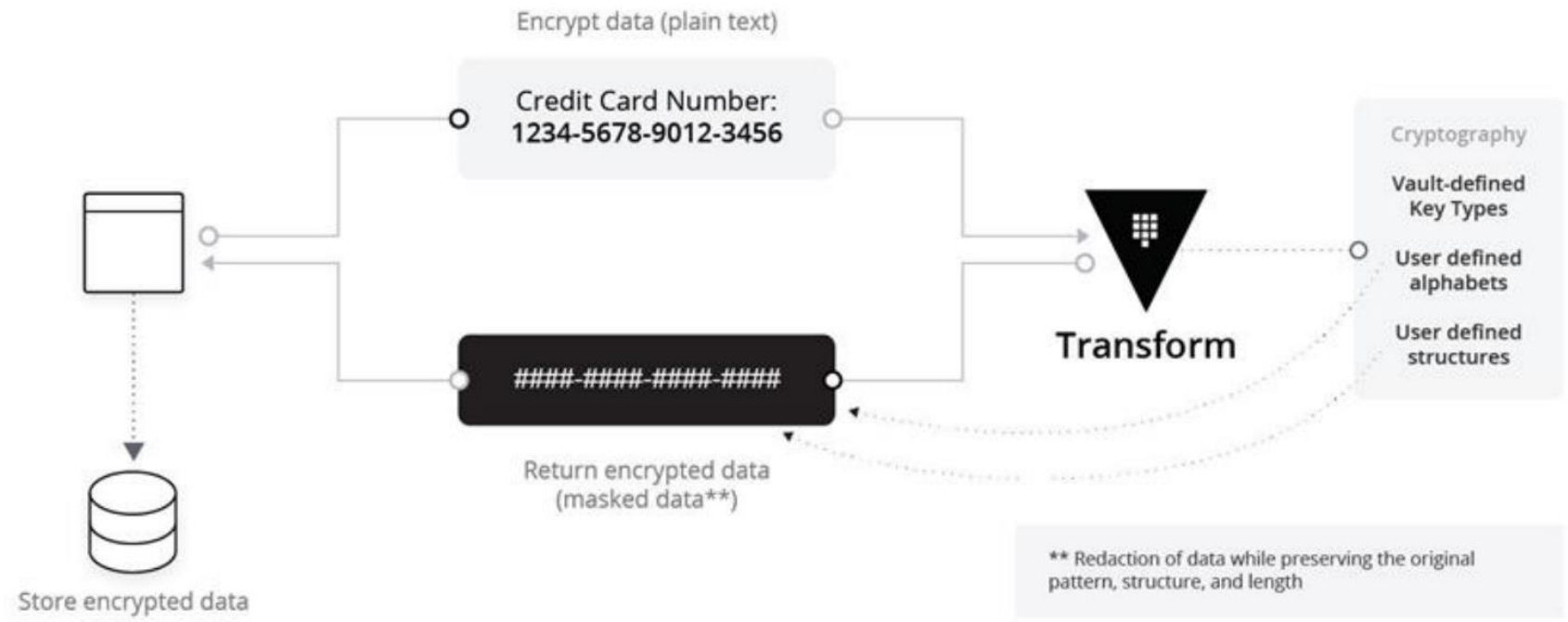


Vault | How Vault Works

DATA TEKNOLOGI SEMESTA

Data Masking

Transform Secrets Engine

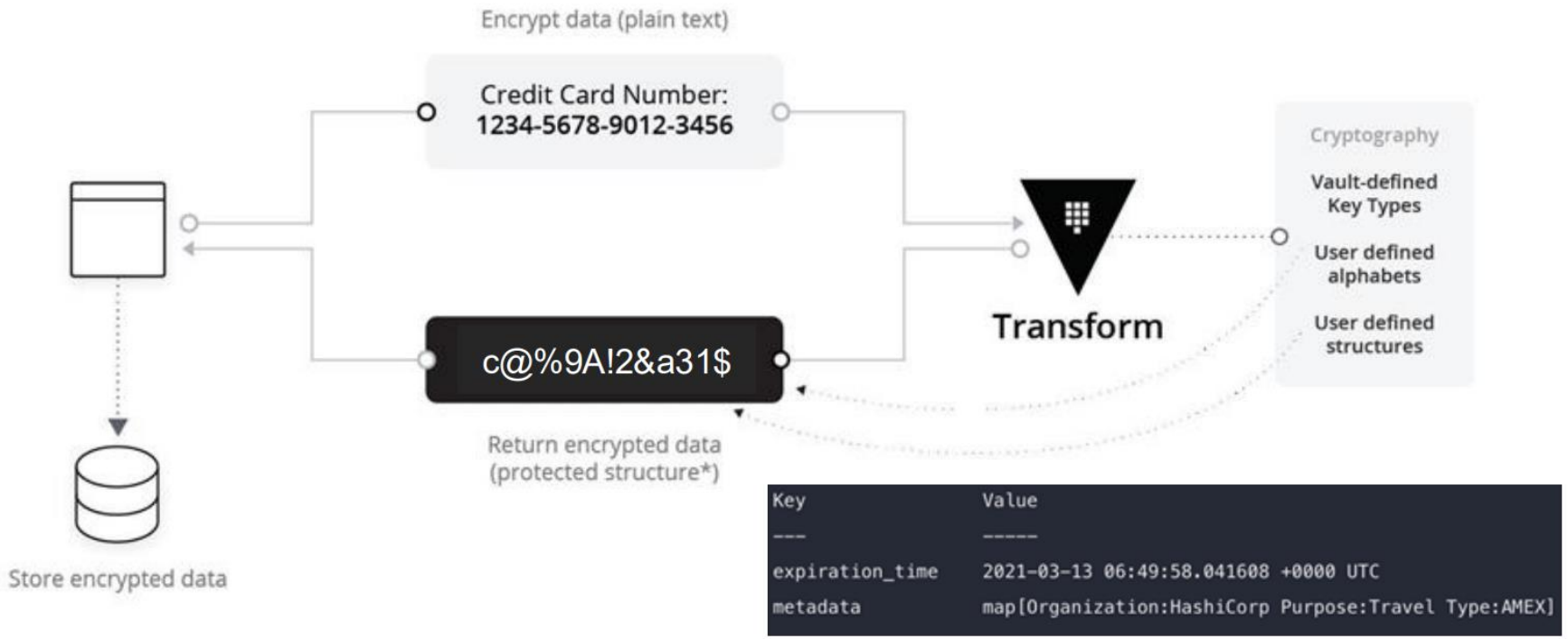


Vault | How Vault Works

DATA TEKNOLOGI SEMESTA

Tokenizations

Transform Secrets Engine



Vault | How Vault Works

DATA TEKNOLOGI SEMESTA

Vault Encryption as a Services

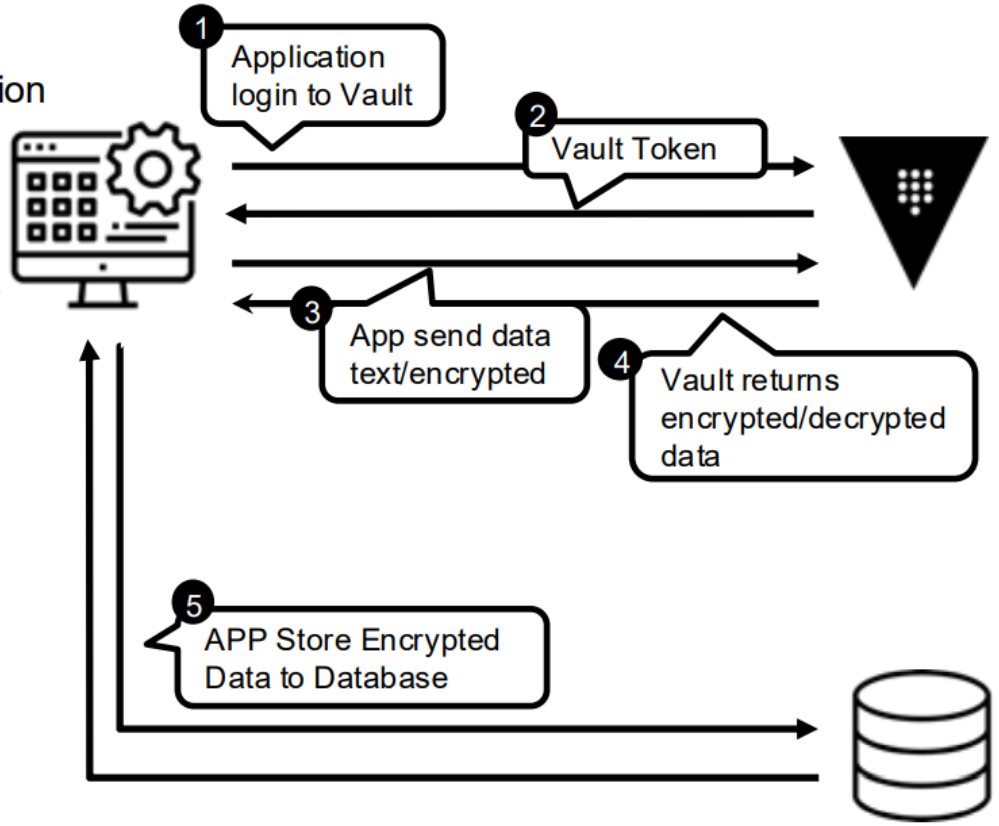
FPE - Format Preserving Encryptions, Masking, Tokenization

→ Automate encryption, decryption, and cryptographic hashing and signing without deploying new infrastructure

→ Keep application data secure with one centralized workflow to encrypt and tokenize data in flight and at rest

→ Quickly create and manage keys (including rotation) without deploying complex key management servers

→ Support AES 256, RSA (2048 and 4096), ECDSA-p256, ed25519, chacha20-poly1305, and more.



DATA TEKNOLOGI SEMESTA

CONTACT US

BELLEZZA BSA 1ST FLOOR UNIT 106
JL. LETJEN SOEPENO - KEBAYORAN LAMA,
JAKARTA SELATAN 12210
INDONESIA

+62 21 50106260 ext.622/625

sales@ptdts.co.id