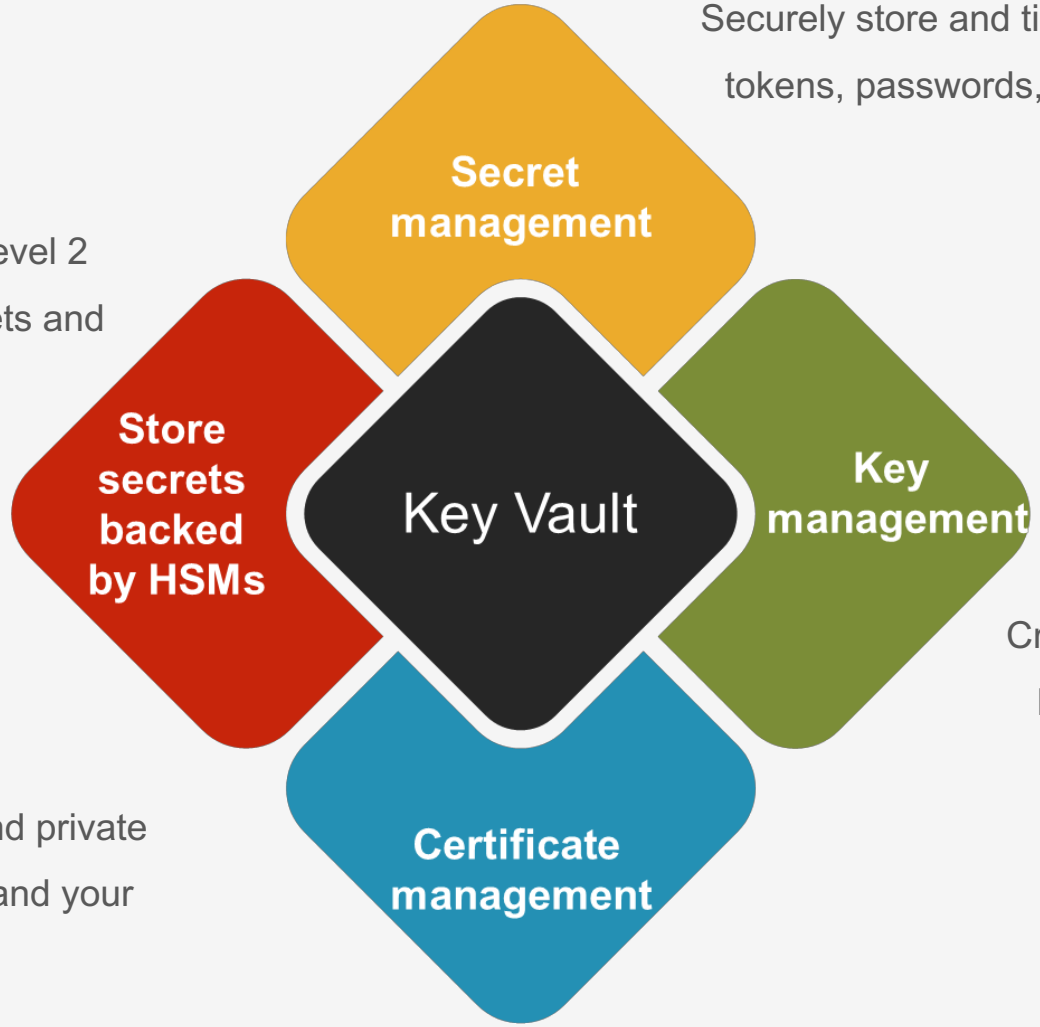
Introduction to Azure Key Vault

Azure Key Vault overview

Azure Key Vault is a service for securely managing Keys, secrets, certificates and any other critical confidential information.

Securely store and tightly control access to tokens, passwords, certificates, API keys, and other secrets..

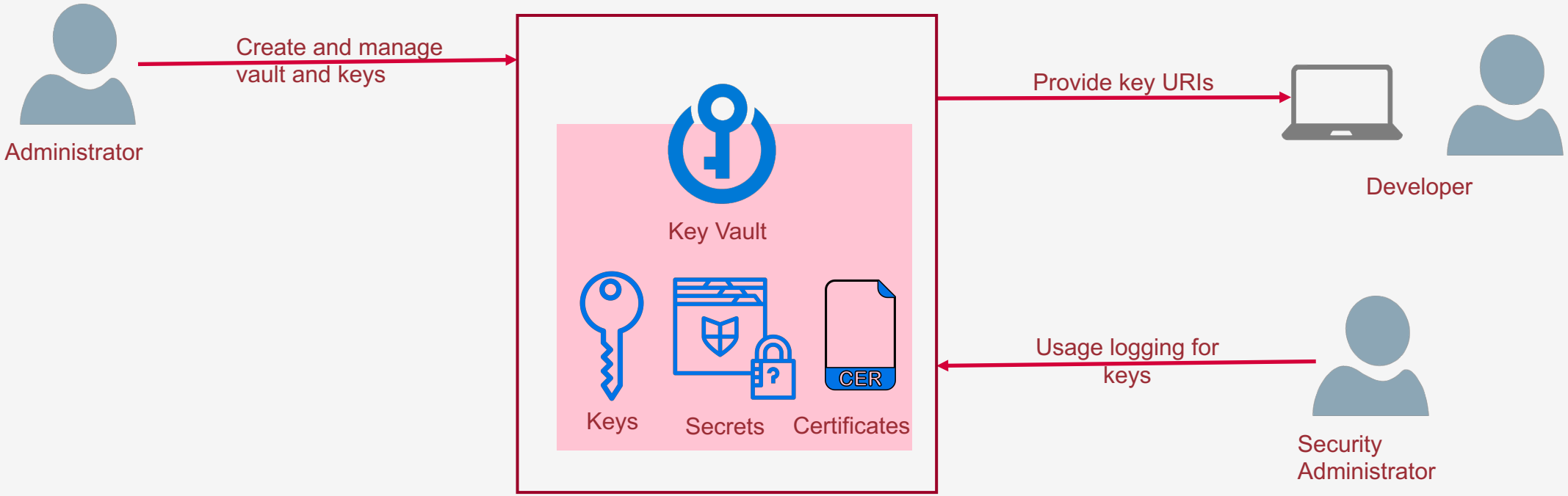
Use either software or FIPS 140-2 Level 2 validated HSMs to help protect secrets and keys.



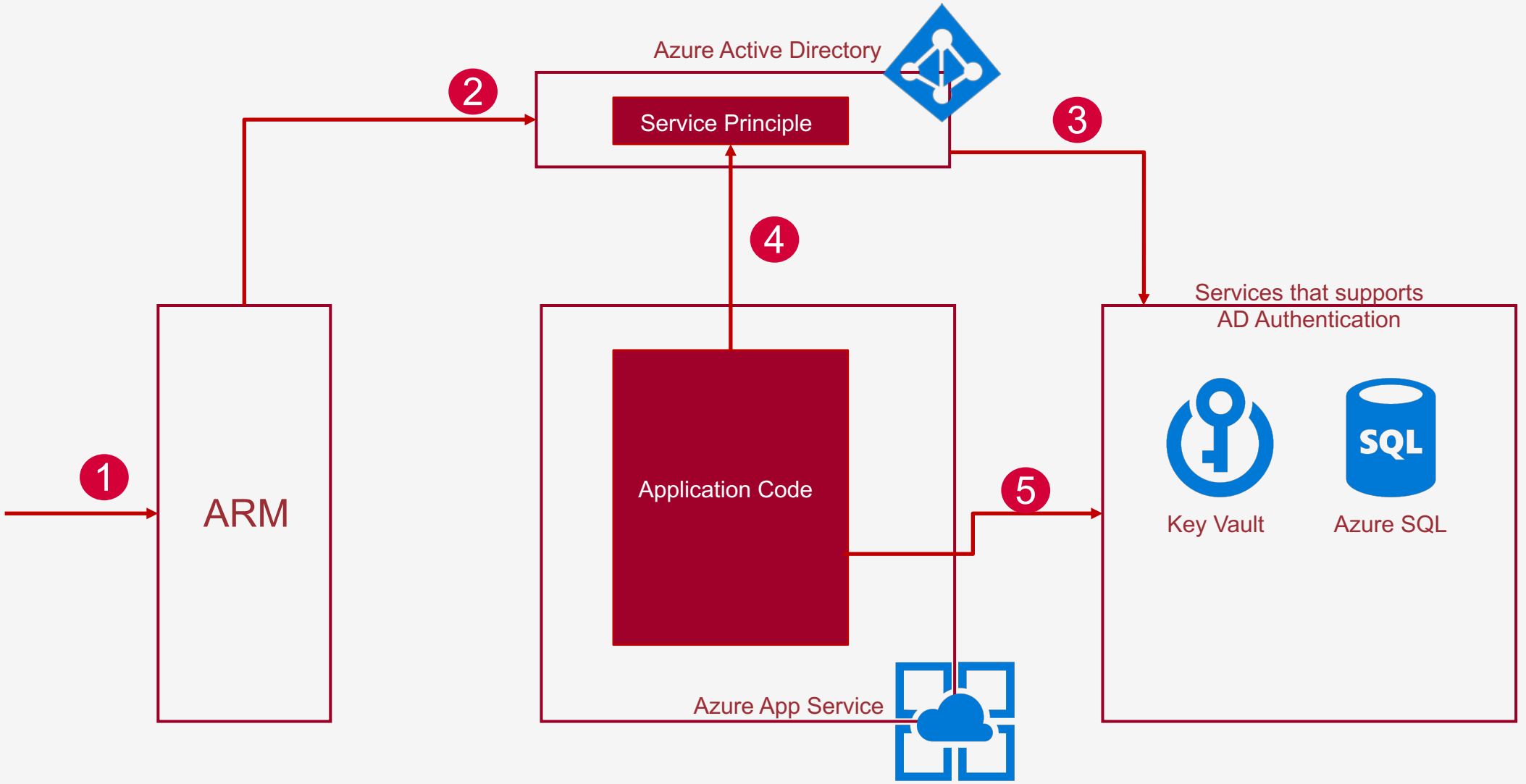
Create and control encryption keys that encrypt your data.

Provision, manage, and deploy public and private SSL/TLS certificates for use with Azure and your internal connected resources.

Key vault usage approach



Azure Key Vault usage best practice

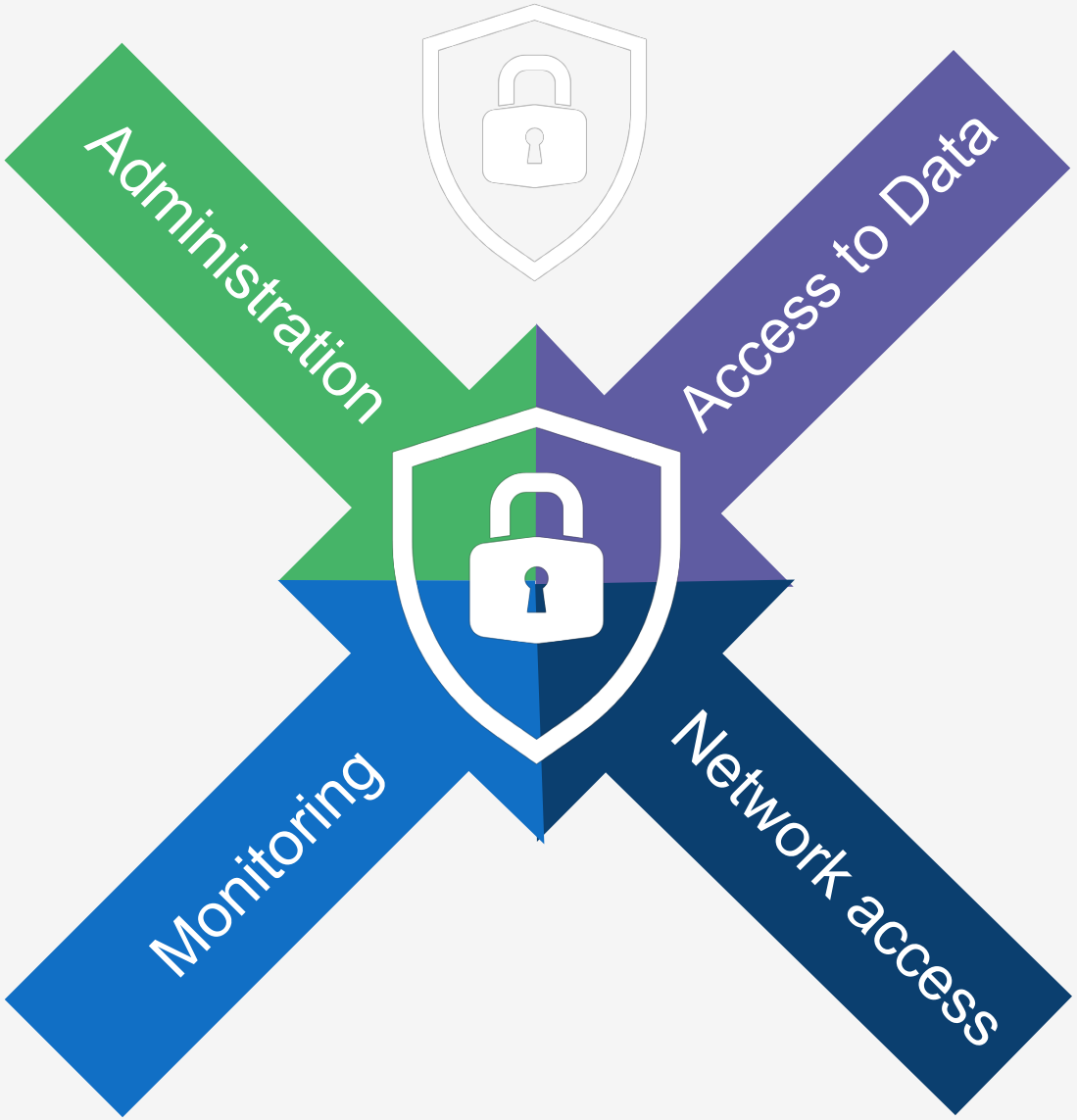


Key vault security

RUDRA PRODUCTS & SERVICES

01

The management plane is where you manage Key Vault itself and it is the interface used to create and delete vaults. You can also read key vault properties and manage access policies.



02

Key Vault access policies grant permissions separately to keys, secrets, or certificate. Access permissions for keys, secrets, and certificates are managed at the vault level.

04

Key Vault logging saves information about the activities performed on your vault. Logging information can be accessed within 10 minutes after the key vault operation

03

You can reduce the exposure of your vaults by specifying which IP addresses have access to them. The virtual network service endpoints for Azure Key Vault allow you to restrict access to a specified virtual network.