

Data-at-Rest Encryption Architecture Overview

1. Introduction

Data-at-rest encryption is the process of encrypting stored data to prevent unauthorized access or exposure. This document provides an overview of a typical Data-at-Rest Encryption Architecture.

2. Key Components

- 1. Data Storage Systems
Any system or service where sensitive data is stored, such as file systems, databases, and object storage.
- 2. Encryption/Decryption Module
Handles cryptographic operations to secure and retrieve information.
- 3. Key Management Service (KMS)
Centralized system responsible for the creation, storage, rotation, and deletion of encryption keys.
- 4. Access Policy Controller
Defines and enforces policies governing access to cryptographic keys and encrypted data.

3. Data Flow

- 1. User or application issues a read/write operation to the storage system.
- 2. On write, data is encrypted by the Encryption Module before being stored to disk.
- 3. Encryption keys are fetched securely from the KMS according to policy.
- 4. On read, stored data is decrypted by the Encryption Module using the key fetched from KMS.
- 5. Decrypted data is returned to the user or application.

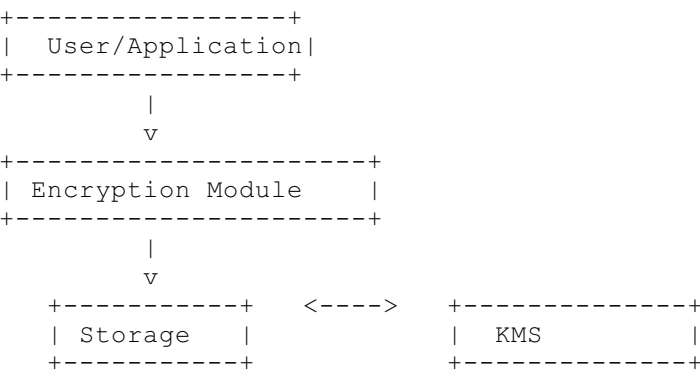
4. Key Management Lifecycle

- **Key Generation:** KMS generates cryptographically strong keys for encryption.
- **Key Storage:** Keys are securely stored within KMS, inaccessible to general storage systems.
- **Key Usage:** The Encryption Module requests keys as needed, according to enforced access policies.
- **Key Rotation:** Keys are rotated periodically to reduce exposure.
- **Key Deletion:** Expired or compromised keys are securely destroyed.

5. Security Considerations

- Separation of duties between those managing storage and those managing keys.
- Audit logging of key access and usage operations.
- Strong access controls and authentication for all KMS operations.
- Regular testing and validation of cryptographic controls.

6. Diagram (Sample)



Summary

Data-at-Rest Encryption ensures that stored data remains secure and unreadable without authorized key access, leveraging centralized key management and secure cryptographic practices.