<p>| | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Key Management Refresher</td>
<td>5</td>
<td>Deployment of a Key Management Lifecycle Solution</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Deep Dive into the Key Lifecycle</td>
<td>6</td>
<td>Software-based HSM Overview Deployment Approach</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Key Lifecycle Phases and Features</td>
<td>7</td>
<td>Industry Specific Differences</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Planning for a Key Management Lifecycle Solution</td>
<td>8</td>
<td>On-Premises Considerations</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Overview

• A guideline for enterprise technologists and service providers to manage cryptographic keys effectively and securely throughout the lifecycle, protect digital assets and maintain regulatory compliance.

• Provides guidance, procedures, and important considerations for the secure management of cryptographic keys at every stage of the key lifecycle, regardless of the type of encryption algorithms or keys.

Who is it for?

• Enterprise and security architects,
• Information security specialists,
• Compliance and regulatory experts,
• Legal team,
• Developers,
• System and network administrators, and
• Operations specialists.

Also, security leaders and managers who want to understand the overview of the key management phases and need to make technology decisions related to key management.

Consumers from all industries, government, and public sectors involved in cryptographic activities to secure the confidentiality, availability, and integrity of digital assets.
Key Management Refresher

Encryption Overview

- Cryptographic Algorithms and Keys
- Crypto-Agility

<table>
<thead>
<tr>
<th></th>
<th>CSP Managed Keys</th>
<th>Customer Managed Keys</th>
<th>Customer Held Keys</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key Generation</td>
<td>CSP</td>
<td>Customer</td>
<td>Customer</td>
</tr>
<tr>
<td>Key Distribution</td>
<td>CSP</td>
<td>Customer</td>
<td>Customer</td>
</tr>
<tr>
<td>Key Rotation</td>
<td>CSP</td>
<td>Customer</td>
<td>Customer</td>
</tr>
<tr>
<td>Key Use</td>
<td>CSP</td>
<td>CSP/ Customer</td>
<td>CSP/ Customer</td>
</tr>
<tr>
<td>Key Storage</td>
<td>CSP</td>
<td>CSP</td>
<td>Customer</td>
</tr>
<tr>
<td>Key Revocation</td>
<td>CSP</td>
<td>Customer</td>
<td>Customer</td>
</tr>
<tr>
<td>Key Backup</td>
<td>CSP</td>
<td>Customer</td>
<td>Customer</td>
</tr>
<tr>
<td>Key Auditing</td>
<td>CSP</td>
<td>Customer</td>
<td>Customer</td>
</tr>
<tr>
<td>Availability</td>
<td>CSP</td>
<td>Customer</td>
<td>Customer</td>
</tr>
<tr>
<td>Performance</td>
<td>CSP</td>
<td>CSP</td>
<td>Customer</td>
</tr>
</tbody>
</table>

Table: Shared Responsibility Model

KMS Overview

- Cloud Native KSM
- Cloud Service Provider Managed Keys
- Customer Managed Keys
- Customer Held Keys
Figure 1. Cloud and on-premises KMS patterns (Ref: CSA document - key management in Cloud Services).
Dive into Each Item in the Key Management Lifecycle and Features

Key Roles and Responsibilities:

- **KMS Administrator:**
  - Manages and configures the KMS system
  - Ensures proper access controls and permissions for key management

- **Key Generator:**
  - Generates cryptographic keys with sufficient entropy.
  - Ensures keys are generated using approved algorithms and lengths

- **Key Custodian:**
  - Safely stores and manages keys throughout their lifecycle
  - Handles key distribution, rotation, and destruction

- **Key User:**
  - Uses keys for cryptographic operation in authorized applications
  - Complies with key usage policies and security best practices

- **Auditor:**
  - Conducts regular audits to ensure compliance and identify vulnerabilities
  - Reviews key management practices for security and efficiency

- **Compliance Officer:**
  - Ensures that KMS aligns with relevant regulatory requirements and standards
  - Maintains compliance with data protection and privacy regulations

- **System Administrator:**
  - Manages and maintains the KMS infrastructure, including hardware and software components
  - Ensures the availability and reliability of the KMS system.
Planning for a Key Management Lifecycle Solution

• **Technical Considerations:**
  - Design a key management strategy to define the purpose of the keys and the consumers’ capabilities.
  - Effective generation of keys to avoid predictivity.
  - Assessment of encryption algorithms and key sizes before planning for use.
  - Selection of correct encryption algorithm and key size.
  - Improvement of the security of the cryptosystem.
  - Multiple regions and availability zones employment to improve availability and fulfill disaster and recovery requirements for cloud-based systems.
  - Safeguard and recover the keys plan in case of loss or damage.
  - Secure transport mechanisms while accessing the KMS and keys.
  - Logging, monitoring, and reporting available in the KMS solution.
  - Integration with other required systems.

• **Operational Considerations:**
  - Physical security.
  - Use of Hardware Security Modules.
  - Take advantage of the key management services offered by multiple cloud service providers.
  - Key incident response plan.

• **Financial Considerations for On-Prem & Multi-Cloud:**
  - Initial Set-up costs
  - Operating expenses
  - Scalability costs
  - Vendor lock-in
  - Data transfer costs
  - Compliance and regulatory costs
  - Disaster Recovery and Redundancy
  - Training and Skill Development
  - Total Cost of Ownership (TCO) Analysis
  - Economic models
  - ROI and business value.

• **Best Practices for the Implementation:**
  - Pilot project
  - Key stakeholders and IT personnel
  - Comprehensive testing during the pilot phase
  - Scaling up the implementation
  - Continuous monitoring and adaptation
  - Iterative improvement.
Deployment of a Key Management Lifecycle Solution

Hardware-Based HSM Deployment Approach.
- Deployment Approach for HSM
- Deployment in the cloud.
- Hybrid environment
- HSM-as-a-service mode
- Software-Based HSM Overview Deployment Approach
- Deployment Approach for Software-Based HSM with Cloud Service Provider Keys

Operations and Maintenance:
- Change management process and plan
- System compatibility, scalability and integration
- Security requirements
- Pilot or small-scale deployments for feedback
- Testing to existing systems
- Documentation of configuration settings, version control and customization.

Deployment Considerations:
- Identity and access management.
- Network security
- Auditing
- Integrations and protocols
- Key management interoperability protocol (KMIP)
- Availability
- Scalability
- Security review
- Trusted computing
- Testing and validation

Auditing Requirements:
- Compliance
- Logging
  - Logged source
  - Logged activities
  - Logged contents
  - Log integrity and retention
  - Log monitoring
- Preparation
  - Architecture
  - Documentation
- Deployment and management
On-Premises Considerations

- Physical Control
- Data Sovereignty and Residency Requirements
- Latency and Performance
- Redundancy and Availability
- Scalability
- Maintenance and Patching
- Support Staff
- Cost

- Security Controls
- Integration with Existing Infrastructure
- Customization and Flexibility
- Auditability and Compliance
- Risk Mitigation
- Data Privacy
- Organizational Policies
- Hybrid Deployments
Industry Specific Differences

1. Financial - Payment Card Industry - Data Security Standard (PCI-DSS)

2. Health Insurance Portability and Accountability Act (HIPAA)

3. Defence and military sectors

4. The NATO standard for secure communication protocols and cryptographic techniques
Cloud Key Management working group

CSA page: https://cloudsecurityalliance.org/research/working-groups/cloud-key-management/

Circle community: https://circle.cloudsecurityalliance.org/community-home?communitykey=7e44948d-7698-4471-994b-33ea8766b5de

Other publications:

- Key Management in Cloud Services
- Recommendations for using a Customer Controlled Key Store
- Cloud Key Management System with External Origin Key
- Recommendations for Adopting a Cloud-Native Key Management Service