PCI Security Standards Council®

2025 ASIA-PACIFIC COMMUNITY MEETING

2025 ASIA-PACIFIC COMMUNITY MEETING

Beyond Encryption:

Key Management as a Strategic Enabler

PCI Security Standards Council®

Sachin Sawant

QSA, CISA, CISM

SVP - Compliance and Testing

SISA

PCI Security Standards Council

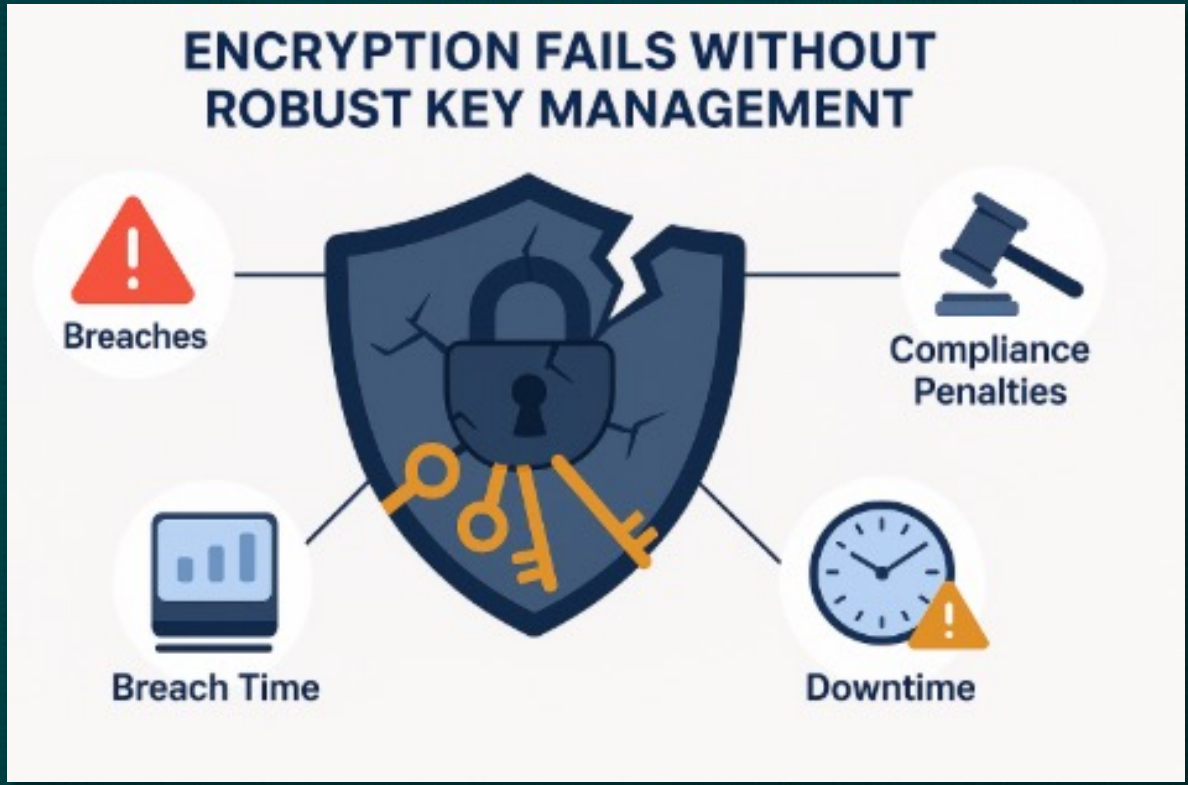
Agenda

- Setting the Stage: The Alarming Truth About Key Management
- Real-World Impact: Lessons from High-Profile Breaches
- Key life-cycle management
- Strategic Framework
- Beyond Compliance: Building a Secure & Agile Organization
- Modern Toolkit: Key Management Technologies
- Aligning Security with Business Objectives
- Future Trends
- Strategic Takeaways

The Alarming Truth About Key Management

SECURITY SPEND IS SOARING; BUT BREACHES ARE RISING EVEN FASTER

While organizations invest heavily in encryption to protect sensitive data, the effectiveness of encryption fundamentally depends on how well cryptographic keys are managed.



PCI Security Standards Council

Lessons Learned from Breaches

Rise of Data Breaches:

- **Retail Chain Data Breach (July 2025)** – Encrypt sensitive customer and employee data at rest, and isolate keys from the data they protect.
- **Luxury Brand Breach (July 2025)** – A reported cyberattack targeted internal systems, potentially exposing employee and customer data. Without proper segregation of encryption keys and access layers, attackers can pivot internally after initial access.
- **Ride-Sharing Platform Breach (2022)** – Avoid hard-coding credentials or secrets; instead, securely store keys in vaults and ensure their management, rotation, and auditing.

Lessons Learned from Breaches

Rise of Data Breaches:

- **Open-Source Library Vulnerability (2021)** – Zero-trust access to key management systems is essential. Just patching vulnerabilities isn’t enough; protect backend systems (like KMS) with strict network and identity controls to prevent lateral movement.
- **Supply Chain Attack (2020)** – Keys should not be accessible to compromised systems by default. Implement role-based access controls (RBAC), enforce key usage logging, and monitor for anomalous decryption requests.

Key Lifecycle Management

Key Generation

- Use strong entropy such as Secure RNG (FIPS Certified)
- -Key size: AES-256, RSA-4096
- Generate Keys Inside Secure Boundaries

Distribution and Access Controls

- Secure channels (TLS 1.2+)
- RBAC: Custodians, Users, Auditors
- IAM integration

Secure Storage

- PCI DSS Req 3
- HSMs: FIPS 140-2/3 compliant
- Cloud Key Vault

Key Rotation and Expiry

- Rotation frequency (e.g., annually)
- Rollback & re-encryption planning
- Application support is critical

Key Destruction

- Follow PCI DSS and NIST 800-88
- Use validated-approved tools
- Maintain destruction logs

Governance

- Access Control: Principle of least privilege
- Approval Workflow: No key change should happen without formal review
- Auditability: All actions must be logged and reviewable

PCI Security Standards Council

Key Lifecycle Management

Key Generation

- Use strong entropy such as Secure RNG (FIPS Certified)
- -Key size: AES-256, RSA-4096
- Generate Keys Inside Secure Boundaries

Distribution and Access Controls

- Secure channels (TLS 1.2+)
- RBAC: Custodians, Users, Auditors
- IAM integration

Secure Storage

- PCI DSS Req 3
- HSMs: FIPS 140-2/3 compliant
- Cloud Key Vault

Key Rotation and Expiry

- Rotation frequency (e.g., annually)
- Rollback & re-encryption planning
- Application support is critical

Key Destruction

- Follow PCI DSS and NIST 800-88
- Use validated-approved tools
- Maintain destruction logs

Governance

- Access Control: Principle of least privilege
- Approval Workflow: No key change should happen without formal review
- Auditability: All actions must be logged and reviewable

PCI Security Standards Council

Live Key Rotation: Challenges and Mitigation Strategies

1. Downtime Risks: Rotation may require service restarts or maintenance windows, risking disruption to live systems.
2. Re-encryption Overhead: Bulk re-encryption of data can strain system resources, impacting performance and user experience.
3. Staggered vs. Bulk Rotation: Choosing between gradual (safer) vs. all-at-once (faster) rotation strategies introduces complexity.
4. Backward Compatibility: Systems must handle legacy data encrypted with old keys to ensure seamless access post-rotation.
5. Human Error: Manual processes during rotation can lead to configuration mistakes or key mismatches, increasing security risk.

Strategy Framework

Direct and Action Oriented

By embedding key management into a strategic framework — one that automates governance, enforces rotation, and aligns with compliance mandates — we can turn vulnerability into resilience

PCI Security Standards Council

Strategy Framework

Direct and Action Oriented

By embedding key management into a strategic framework — one that automates governance, enforces rotation, and aligns with compliance mandates — we can turn vulnerability into resilience

PCI Security Standards Council

Compliant Org vs Secure & Agile Org

Aspect	Compliant Organizations	Secure & Agile Organizations
Primary Focus	Meeting regulations and audit requirements	Proactive security integrated with business agility
Key Management	Manual or scheduled rotations (basic)	Automated, policy-driven rotations with zero downtime
Encryption Approach	Minimum standards (AES-256, TLS)	Hardware-backed keys (HSMs), zero-knowledge storage
Crypto Agility	Static algorithms; change only when mandated	Designed for quick algorithm/key upgrades
Monitoring	Periodic reviews and compliance checks	Continuous monitoring with anomaly detection
DevOps Integration	Security added post-deployment	Built-in security in CI/CD pipelines (code signing)
Risk Strategy	Reactive – responds to regulations	Proactive – anticipates emerging threats

The Modern Toolkit

Key Management Technologies

Hardware Security Modules (HSMs):

- Examples: CloudHSM, PCI PTS Certified Hardware HSM's
- FIPS 140-2/3 certified for key generation and protection

Cloud-Native KMS Platforms:

- Cloud Key Management Systems
- Integrated IAM, auto-rotation, global key distribution

Third-Party Centralized KM Solutions:

- HashiCorp Vault, Fortanix DSM, CyberArk
- RESTful APIs, multi-tenant support, policy-based key access

Align Cryptographic Operations with Business Objectives

1. Business Continuity - Ensure systems stay available during security processes.
2. Regulatory Compliance – Meet PCI DSS, Hi-Trust, etc
3. Risk Reduction - Minimize data breach and insider threats
4. Performance & Cost Optimization - Avoid high operational overhead while securing data
5. Customer Trust - Preserve brand reputation and ensure secure transactions.

Align Cryptographic Operations with Business Objectives

1. Business Continuity - Ensure systems stay available during security processes.
2. Regulatory Compliance – Meet PCI DSS, Hi-Trust, etc
3. Risk Reduction - Minimize data breach and insider threats
4. Performance & Cost Optimization - Avoid high operational overhead while securing data
5. Customer Trust - Preserve brand reputation and ensure secure transactions.

Future Trends

Staying Ahead of the Curve

- **AI-Powered Anomaly Detection:** Machine learning models are being trained to detect unusual key usage patterns, helping identify potential misuse or compromise in real time.
- **Quantum-Safe Algorithms:** Adoption of post-quantum cryptography
- **Confidential Computing:** Using secure enclaves (e.g., Intel SGX, AMD SEV) to isolate key operations from host OS, ensuring runtime data protection.

Strategic Takeaways

Your Path to Secure Key Management

- Draft a comprehensive Key Management Policy
- Adopt centralized KMS / HSM use
- Implement a Zero Trust security model where keys are accessible only on a need-to-use basis
- Automate key rotation and access logs
- Integrate key management into CI/CD pipelines for automation
- Enforce RBAC and log all access
- Periodic reviews and simulated drills - Use continuous monitoring tools to trigger alerts before key expiry or policy violations.
- Cross-Training and Awareness
- Compliance Dashboards: Visualize key lifecycle, access logs, and compliance status (PCI DSS, ISO 27001) via tools for audit readiness.

Strategic Takeaways

Your Path to Secure Key Management

- Draft a comprehensive Key Management Policy
- Adopt centralized KMS / HSM use
- Implement a Zero Trust security model where keys are accessible only on a need-to-use basis
- Automate key rotation and access logs
- Integrate key management into CI/CD pipelines for automation
- Enforce RBAC and log all access
- Periodic reviews and simulated drills - Use continuous monitoring tools to trigger alerts before key expiry or policy violations.
- Cross-Training and Awareness
- Compliance Dashboards: Visualize key lifecycle, access logs, and compliance status (PCI DSS, ISO 27001) via tools for audit readiness.

Thank You

PCI Security Standards Council