

Service Name

AWS Payment Cryptography

Service Overview

AWS Payment Cryptography is a managed service that provides access to cryptographic functions and key management for payment processing in compliance with PCI standards without requiring dedicated payment HSM instances. The service enables payment functions like acquirers, payment facilitators, networks, switches, processors, and banks to move cryptographic operations closer to cloud applications while minimizing dependencies on auxiliary data centers. It leverages PCI PTS HSM V3 and FIPS 140-2 Level 3 certified hardware with low latency and high availability, eliminating operational requirements of on-premises HSMs such as hardware provisioning, key material management, and emergency backup maintenance.

Key Use Cases

- Card issuing operations: EMV PIN change, cardholder-selectable PINs, PIN reveal, CVV/CVV2 generation and validation, and ARQC processing for transaction authorization
- Acquiring and payment facilitation: Data decryption from payment terminals using TDES, AES, and DUKPT techniques with PCI P2PE compliance, PIN translation between encryption keys, and MAC verification for data integrity
- Key exchange and synchronization: Electronic key sharing with partners using TR-34, TR-31, and ECDH protocols, eliminating manual paper-based key component sharing and enabling secure migration from on-premises HSMs

Features

- **Key Management:** Create, manage, import, and export symmetric and asymmetric keys (TDES, AES, RSA) with alias management, tagging, and TR-31/TR-34 support
- **Cryptographic Operations:** Encrypt, decrypt, re-encrypt data, generate/validate CVV/CVV2/ARQC, PIN translation, MAC generation/verification, and cardholder data processing
- **Multi-Region Replication:** Automatic key replication across AWS regions for high availability, disaster recovery, and global operations with consistent key IDs
- **PCI Compliance:** Built-in compliance with PCI PIN, PCI P2PE, and PCI DSS standards using PCI PTS HSM V3 certified hardware
- **Electronic Key Exchange:** Support for TR-34, TR-31, and ECDH protocols for secure electronic key exchange with partners and HSM synchronization
- **Post-Quantum Security:** Hybrid post-quantum TLS support using ML-KEM cryptography for securing API calls against future quantum computing threats

Value Proposition

AWS Payment Cryptography eliminates the operational complexity and costs of managing on-premises payment HSMs while providing elastic scalability and built-in PCI compliance. The service offers significant advantages over traditional solutions including elimination of hardware provisioning, maintenance, and emergency backup requirements in secure facilities:

- Customers benefit from industry-leading availability SLAs, automatic failover between availability zones, and the ability to electronically share keys with partners instead of using paper-based processes
- The service provides cost optimization through tiered pricing models and reduces total cost of ownership compared to dedicated HSM infrastructure
- Integration with AWS services enables modern cloud-native payment architectures with API-based operations and faster time-to-market for payment applications

Service Integration

AWS Payment Cryptography integrates deeply with core AWS security and monitoring services for comprehensive payment processing solutions. Primary integrations include AWS Identity and Access Management (IAM) for authentication, authorization, and access control policies with support for dual control operations:

- AWS CloudTrail provides comprehensive audit logging for all key management and cryptographic operations, while Amazon CloudWatch enables monitoring and alerting
- The service supports Amazon VPC and AWS PrivateLink for secure network connectivity, and AWS Direct Connect for dedicated network connections
- Integration with AWS Key Management Service (KMS) and AWS CloudHSM provides additional cryptographic options for complementary use cases, enabling customers to build complete payment security architectures across multiple AWS security services

Onboarding and Offboarding

Customers get started by ensuring proper IAM permissions and installing the AWS CLI, SDKs, or using AWS APIs for service access. The onboarding process begins with creating cryptographic keys using the Control Plane API, specifying key attributes like algorithm (TDES, AES, RSA), usage (CVV generation, PIN translation, etc.), and key modes of use:

- The Getting Started tutorial demonstrates creating a CVK key for CVV2 operations, followed by cryptographic operations using the Data Plane API
- AWS provides comprehensive workshops, GitHub samples, and documentation to help customers explore deployment patterns and common use cases

- Customers can import existing keys from on-premises HSMs using TR-31 and TR-34 protocols or create new keys within the service, with immediate access to cryptographic operations upon successful key creation

Getting Started Guide: <https://docs.aws.amazon.com/payment-cryptography/latest/userguide/getting-started.html>

Data Removal

Key deletion in AWS Payment Cryptography involves scheduling keys for deletion with a configurable waiting period (3-180 days, default 7 days) during which keys enter DELETE_PENDING state and cannot be used for cryptographic operations. Deletion is irreversible and permanently removes key material and metadata, making decryption of previously encrypted data impossible. Customers can cancel deletion before the scheduled time using the restore-key operation. For Multi-Region keys, deleting a Primary Region key automatically deletes associated Replica Region keys across all replication regions, ensuring complete data removal.

Backup/Restore and Disaster Recovery

AWS Payment Cryptography provides built-in high availability and disaster recovery through Multi-Region key replication, automatically distributing keys across AWS regions with eventual consistency. The service maintains durability matching AWS's highest durability services and operates across at least three availability zones per region with automatic failover. Key material is protected by HSM AES 256 main keys and stored in encrypted databases with replication to in-memory databases on Payment Cryptography servers, ensuring resilience against hardware failures and regional outages.

Backup Capabilities

AWS Payment Cryptography does not integrate with AWS Backup as it manages key material internally through HSM-based protection and encrypted storage. The service provides inherent backup through Multi-Region replication capabilities, cross-region key synchronization using TR-34 and TR-31 protocols, and durable key storage protected by regional and profile main keys. Key durability is designed to match AWS's highest durability services with automatic replication across availability zones within each region.

Disaster Recovery

The service does not integrate with AWS Elastic Disaster Recovery but provides native disaster recovery through Multi-Region key replication and regional isolation design. AWS Payment Cryptography supports automatic failover between availability zones with zero planned downtime and cross-region key distribution for business continuity. The service enables customers to implement custom disaster recovery solutions using the cross-region replication capabilities and industry-standard key exchange protocols for maintaining operational resilience.

Recovery Objectives

AWS Payment Cryptography helps customers achieve aggressive RPO and RTO objectives through Multi-Region key replication with near real-time synchronization and automatic availability zone failover. The service's regional isolation design and elastic scaling capabilities enable customers to maintain cryptographic operations during regional outages by utilizing replicated keys in secondary regions. High availability SLAs and low-latency operations support critical payment processing requirements with minimal recovery time objectives for business-critical payment functions.

Service Constraints

Service Quotas: <https://docs.aws.amazon.com/payment-cryptography/latest/userguide/quotas.html>

FAQ: <https://aws.amazon.com/payment-cryptography/faqs/>

Technical Requirements

Service Documentation: <https://docs.aws.amazon.com/payment-cryptography/latest/userguide/what-is.html>

User Guide: <https://docs.aws.amazon.com/payment-cryptography/latest/userguide/>

API Reference: <https://docs.aws.amazon.com/payment-cryptography/latest/APIReference/Welcome.html>

Pricing Overview

Please see the AWS UK G Cloud 15 Pricing Document accompanying this service in the Digital Marketplace.

Public Pricing: <https://aws.amazon.com/payment-cryptography/pricing/>

Cost Optimization

AWS Payment Cryptography offers unique cost optimization through recent pricing reductions of up to 63% for API requests and introduction of tiered key pricing models that scale with volume. The service eliminates traditional HSM hardware costs including procurement, maintenance, facility requirements, and dedicated personnel:

- Customers benefit from elastic scaling that charges only for actual usage rather than provisioned capacity, and Multi-Region replication reduces the need for separate disaster recovery infrastructure
- The tiered pricing structure enables cost-effective scaling for high-volume cryptographic operations while the managed service model eliminates operational overhead costs associated with on-premises HSM management and PCI compliance maintenance

Savings Considerations

Primary cost savings derive from eliminating dedicated payment HSM infrastructure, including hardware acquisition, data center colocation, secure facility requirements, and specialized technical personnel. The managed service model removes ongoing operational costs such as HSM maintenance, firmware updates, emergency backup management, and PCI compliance auditing overhead:

- Customers save on disaster recovery infrastructure through built-in Multi-Region replication and high availability features
- Electronic key exchange capabilities eliminate costs associated with physical key component transportation and manual key management processes
- The elastic pricing model provides significant savings compared to fixed HSM capacity provisioning, enabling customers to optimize costs based on actual transaction volumes and seasonal payment processing patterns