Validating PQC Compliance for Catalyst

Catalyst from Orbis is committed to providing secure and compliant data-sharing solutions that meet stringent regulatory requirements. This document outlines how Catalyst, hosted on Cloudflare's secure infrastructure, leverages advanced post-quantum cryptographic (PQC) algorithms and integrates with Google Cloud's Hardware Security Modules (HSMs) to ensure the highest levels of data protection, regulatory compliance, and operational efficiency.

Overview of Catalyst and Security Objectives

Catalyst's core mission is to deliver secure, scalable, and compliant data-sharing capabilities tailored to meet the needs of diverse organizations, including those with sensitive national security requirements. By integrating advanced cryptographic technologies, Catalyst protects cryptographic keys with state-of-the-art hardware and software solutions, ensuring resistance against both classical and quantum threats.

Hosting Catalyst on Cloudflare

Cloudflare's robust security infrastructure provides the foundation for Catalyst's secure operations. Key benefits include:

- **NIST-Approved Cryptographic Algorithms:** Cloudflare employs cryptographic modules validated by FIPS 140-2, ensuring compliance with industry and governmental standards.
- **FIPS-Validated Cryptographic Modules:** These modules safeguard the integrity of Catalyst's operations while maintaining strict compliance.
- **Secure Key Management with HSMs:** Cloudflare HSMs perform critical functions such as secure key storage, generation, and management, ensuring that private keys are never exposed outside the hardware environment.
- **Post Quantum Cryptography:** Cloudflare provides certificates and technology capable of Post Quantum Cryptography as the default offering.

Leveraging Google Cloud HSM for Advanced Key Management

Catalyst integrates with Google Cloud's Hardware Security Modules (HSMs) to sign and manage cryptographic keys within the Catalyst environment. Google's HSMs are designed to handle sensitive workloads securely, efficiently, and with compliance in mind.

Key Features of Google Cloud HSM

- **FIPS 140-2 Level 3 Certification:** Ensures compliance with stringent security standards for key management and cryptographic operations.
- **Unified API with Cloud Key Management Service (KMS):** Simplifies the process of managing and using HSM-backed keys across different applications and services.
- **Automatic Scaling and High Availability:** Google's managed clusters of HSMs scale to meet demand, ensuring low latency and high performance without operational overhead.
- **Geographic Control:** Catalyst's integration with Google HSM ensures keys remain securely managed within predefined geographic boundaries, aligning with regulatory requirements.
- **Robust Cryptographic Operations:** Supports a wide range of cryptographic tasks, including signing, encryption, decryption, and attestation, all performed within secure hardware environments.

Catalyst's Cryptographic Model

Catalyst, as a data mesh, provides encryption in transit to all data that transitions the mesh. Catalyst employs both Transportation Layer Security (TLS) and the cryptographic signing of Application Programming Interface (API) keys in the following manner:

- **Transportation Layer Security (TLS):** All data to, from, and across Catalyst is encrypted in transit all of the time.
- **Application Programming Interface (API) Key Signing**: Catalyst utilized cryptographic methods to facilitate verifiable access to data provide through Catalyst.

Integration Workflow

Catalyst's integration with Cloudflare and Google Cloud HSM ensures seamless and secure data-sharing capabilities:

- **Google Cloud HSM Deployment**: Google Cloud HSM is deployed using itself as the root of trust or utilizing an external Certificate Authority to establish an external root of trust.
- **Secure Signing with Google Cloud HSM:** Keys used for cryptographic operations are signed and managed within Google's HSMs, ensuring authenticity and protection against tampering.
- **Secure Communication Channels:** Catalyst establishes secure connections between Cloudflare's infrastructure and Google Cloud HSMs using TLS and using API's which only have the authority to ask for cryptographic signing. Catalyst never has access to the raw key material.

- **API Access and Role-Based Controls:** Fine-grained access control mechanisms, such as mutual TLS (mTLS), role-based access controls (RBAC), and formal restrict access to cryptographic functions, ensuring that only authorized entities can interact with HSMs.

Operational and Compliance Advantages

By combining Cloudflare's infrastructure with Google Cloud HSM's advanced key management, Catalyst delivers:

- **Operational Efficiency:** Automatic scaling and centralized management reduce the complexity of managing cryptographic operations.
- **Regulatory Assurance:** Compliance with FIPS 140-2 Level 3, FedRAMP High, and other industry standards ensures Catalyst meets stringent security requirements.
- **Future-Proof Security:** Integration of post-quantum cryptographic algorithms like Kyber ensures resistance against emerging quantum threats.
- **Flexible Deployment Models:** Catalyst supports both hardware-backed and software-only models, catering to diverse use cases and security needs.

Conclusion

Catalyst, hosted on Cloudflare and integrated with Google Cloud's HSMs, represents a modern, efficient, and secure solution for managing cryptographic keys and protecting sensitive data. By leveraging the strengths of both platforms, Catalyst ensures compliance with the most stringent regulatory requirements while delivering operational excellence and quantum-resistant security.