White paper

Google Bare Metal Rack HSM and Bare Metal HSM

PCI DSS, 3DS, PIN and P2PE Compliance

Sam Pfanstiel | Ph.D., CISSP, CISM, CISA, CEH, QSA, QPA, P2PE Application Assessor, 3DSA, SSF SSA & Secure SLCA

Bhavna Sondhi | CISA, CEH, ISO 27001 Lead Implementer, QSA, QPA, P2PE Application Assessor, 3DSA, SSF SSA & Secure SLCA

COALFIRE

North America | Europe

877.224.8077 info@coalfire.com | Coalfire.com

Table of contents

Executive Summary

Google LLC ("Google") engaged Coalfire Systems, Inc. ("Coalfire"), a respected Payment Card Industry (PCI) Qualified Security Assessor (PCI QSA) company, PCI 3-D Secure (3DS) assessor company, PCI Qualified Personal Identification Number (PIN) Assessor (QPA) company, and PCI Point-to-Point Encryption (P2PE) assessor company to conduct an independent technical assessment of their Google Bare Metal Rack HSM and Bare Metal HSM solutions (collectively, "customer-owned HSM solutions"). Coalfire conducted assessment activities including document reviews, an architectural assessment, production facility site walkthroughs, and staff interviews to validate the physical security controls of the Google Bare Metal Rack HSM and Bare Metal HSM solutions deployed within Google's production facilities.

The goal of this white paper is to discuss the Google Bare Metal Rack HSM and Bare Metal HSM solutions' architectures and how these services can meet some of the applicable physical security requirements within the PCI DSS 4.0, PCI 3DS Core 1.0, PCI PIN 3.1, and PCI P2PE 3.1 standards for their customers. Both Google customer-owned HSM solutions were included in the most recent PCI DSS, PCI 3DS Core, and PCI PIN service provider assessments performed by Coalfire; and, while PCI P2PE program eligibility criteria prevent the validation of infrastructure-as-a-services like Bare Metal Rack HSM and Bare Metal HSM, applicable controls have been similarly assessed and discussed herein. Customers that utilize these solutions may use this white paper and the resources discussed herein to obtain better understanding of responsibilities and assurance of applicable physical security requirements under PCI DSS 4.0, PCI 3DS Core 1.0, PCI PIN 3.1 and PCI P2PE 3.1.

Google Bare Metal Rack HSM and Bare Metal HSM

There are two Google infrastructure-as-a-service (IaaS) offerings that allow customers to host their own HSM equipment in Google Cloud facilities: **Bare Metal Rack HSM** and **Bare Metal HSM**. These services provided by Google enable the deployment of customer-owned HSMs within Google managed colocation facilities, allowing for connectivity of PCI-sensitive workloads with customer-managed cryptographic hardware, directly within Google Cloud infrastructure.

Both services are intended for customers that provide their own HSM devices, which Google will physically install in the Google-controlled space within its secure data center locations. Enterprise customers who have a need for single-tenant HSMs can utilize either service to achieve true "bring-your-own-HSM" architecture.

The primary differences between these services lie in the minimum number of HSMs deployed, placement in shared vs. dedicated racks, and the availability of physical access to the HSMs:

- **Bare Metal Rack HSM**
  - requires at least four new HSMs: deployed in at least two Google Cloud regions, each containing two dedicated racks with at least one HSMs in each rack.
  - intended for enterprises with 100 or more HSMs, allows for customers to schedule escorted physical access to their dedicated racks of HSMs.
- **Bare Metal HSM**
  - requires at least four HSMs: deployed in at least two Google Cloud regions, where HSMs are securely housed in at least two shared racks, each containing at least one HSM.
  - does not allow the customer physical access to the HSMs.

Due to the similarity of these bring-your-own-HSM offerings, and for ease of discussion, where compliance impacts are identical these services will be referred to collectively as "the customer-owned HSM solutions." However, where a distinction may be drawn, these offerings will be referred to by their proper service names, Bare Metal HSM and/or Bare Metal Rack HSM.

Overview of the Customer-owned HSM Solutions

Both customer-owned HSM solutions provided by Google include the receipt and installation of customer-owned HSMs; hosting HSMs in the Google-controlled data center; providing rack space, electrical power, network cabling, and network integration within the colocation facility; and managing the physical security of the devices.

Both customer-owned HSM solutions require the HSMs provided by the customer to be Federal Information Processing Standards (FIPS) 140-2 / 140-3 Level 3 certified or better. PCI 3DS Core Security, PCI PIN and PCI P2PE standards include requirements for the use of PCI PIN Transaction Security (PTS) or FIPS 140-2 / 140-3 Level 3 or higher when HSMs are utilized for cryptographic functions applicable within each standard.

After Google installs the HSMs, the customer must be able to perform all device and encryption key management using remote management capabilities. This includes all aspects of the encryption key lifecycle such as key generation; key distribution, loading, and injection; secure storage; cryptographic period management; rotation; and destruction. Customers are also responsible for the security of the customer's facility for remote non-console connections, as applicable under the applicable standards. For instance, customers are responsible for maintaining the physical security controls for any secure room used for remote clear-text key management functions to the HSM devices hosted in the cloud. Google has no logical access to customer-owned HSMs and is unable to access or change any configurations or manage any encryption keys on the HSMs, and will not perform such tasks on behalf of the customer.

Only the Bare Metal Rack HSM solution allows for scheduling of escorted customer physical access to the HSMs within the secure production environment, which may be suitable for such activities, but only under certain conditions, which are discussed herein.

Audience

This assessment white paper has four target audiences:

1. **PCI DSS Community:** This audience may be evaluating either Google HSM solution as part of a PCI DSS assessment of a merchant or service provider environment. This would include Qualified Security Assessors (QSAs) or Internal Security Assessors (ISAs) conducting a PCI DSS assessment of a merchant or service provider, or internal audit preparing for such an assessment.
2. **PCI 3DS Entities:** This audience would include PCI 3DS entities evaluating either Google HSM solution for use within their organization's 3DS environment (3DE). This would also include 3DS Assessors reviewing the 3DS entity for the PCI 3DS Core Security Standard.
3. **PCI P2PE Solution Providers and Component Providers:** This audience would include PCI P2PE solution providers or component providers evaluating either Google HSM solution for deployment and/or management of key functions in their decryption environments (DE). This audience would also include PCI P2PE Assessors reviewing the solution provider or component provider as part of their PCI P2PE assessment.

4. **PCI PIN Entities:** This audience would include entities responsible for PIN transaction processing of PCI brand accounts, acquiring institutions and agents or other entities directed by a participating payment brand who are evaluating either Google HSM solution for deployment and/or management of key functions in their environments. The audience would also include service providers who are acting on behalf of acquiring organization such as Independent Sales Organizations (ISO) and Encryption Service Organizations (ESO) that provide services related to PIN based payment transactions or cryptographic key management operations; and the Qualified PIN Assessors (QPAs) that perform these assessments.

Coalfire Assessment

Scope

The scope of this review was to assess the security controls provided by Google for hosting of customers' HSMs hosted within Google-controlled facilities for the Bare Metal Rack HSM and Bare Metal HSM solutions. This whitepaper also includes best practice considerations for customers to implement PCI DSS, PCI P2PE, PCI PIN and PCI 3DS compliance.

The focus was primarily on the physical security provided by Google to HSMs managed within its production facilities, and their applicability to the respective requirements for physical security within the PCI DSS, PCI 3DS Core Security, PCI P2PE and PCI PIN standards. The logical management and use of customer-owned HSMs for key management and cryptographic operations are handled entirely by customers and are not in scope for this review. This review covers the physical security and policies and procedures in place by Google for physically handling customer HSMs as part of its Google Bare Metal service offerings.

While Google's responsibilities are limited, the customer is ultimately responsible for relevant compliance responsibilities within their Google Cloud Platform (GCP) -hosted environment, where the systems or applications managing the HSM are deployed. For example, when the customer uses network segmentation to limit the scope of its CDE under PCI DSS, the customer is responsible for deployment and configuration of all security tools, such as Virtual Private Cloud (VPC) configurations and Firewall rules, to provide network isolation. Similarly, while other Google Cloud security services such as Cloud Identity or Cloud Logging may be used to support authentication and monitoring requirements for PCI 3DS, the customer is ultimately responsible for the compliant implementation of their 3DS solution.

General categories of PCI requirements that fall under the customers' responsibility include the following:

- Access controls
- Encryption and key management
- Secure cardholder data storage
- Logging
- Secure software development life cycle
- Vulnerability management
- File integrity monitoring
- Security policies and procedures

This review focused on the following functional areas of Google Bare Metal Rack HSM and Bare Metal HSM solutions, against applicable physical security requirements defined within PCI DSS, PCI 3DS, PCI P2PE, and PCI PIN.

1. Google responsibilities for physical protection of customer-provided equipment: Coalfire performed documentation review, interviews, and onsite observation for assurance of these controls.
2. Google responsibilities for secure receipt, installation and deployment of customer provided equipment within the facility hosting the Google HSM solutions: Coalfire performed documentation review, interviews, and structured walkthroughs for assurance of these controls.
3. Google responsibilities for secure decommissioning of HSM devices when they need to be removed, destroyed, or returned: Coalfire performed documentation review, interviews, onsite observation, and structured walkthroughs for assurance of these controls.
4. Shared responsibilities between Google and their customers for the Google HSM solutions: Coalfire performed documentation review, interviews, and structured walkthrough to confirm that Google does not handle or manage any encryption keys on customer-owned HSMs. All key management functions, including key generation; key distribution, loading, and injection; secure storage; cryptographic period management; rotation; and destruction are handled by the customer through the HSM directly. Customers handle any logical access to HSMs deployed as part of the Google customer-owned HSM solutions and Google is not involved in this process.

PCI DSS Compliance

The scope of Google's PCI DSS compliance responsibility for the Google customer-owned HSM solutions is restricted to certain physical security controls, which are covered under PCI Requirement 9, "Restrict Physical Access to Cardholder Data" and security program requirements, which are covered under Requirement 12, "Support Information Security with Organizational Policies and Programs." Applicable requirements include limiting physical access to the controlled production space, logging of physical access by both Google employees and authorized visitors, protections provided by the secured facility for all production hardware, and policies which ensure monitoring and notification of any physical security breaches. The remaining PCI DSS requirements are the responsibility of the customer.

In some cases, customer-owned HSMs may not store, process, or transmit account data directly (e.g., if they are used only for storing keys, and encryption and decryption of cardholder data is performed outside the HSM). However, if they reside within the defined cardholder data environment (CDE) (e.g., in the same VPC as cardholder data), all applicable security requirements must be applied.

Coalfire has conducted an independent assessment of GCP as a third-party service provider for PCI DSS. Customers using GCP for all or part of their cardholder data environment (CDE) and/or PCI DSS processes may request a copy of the GCP PCI 3DS Attestation of Compliance (AOC) and Responsibility Summary, which detail Google's compliance to applicable controls as a third-party service provider.

If the customer is using Google to host its physical HSM using Google Bare Metal Rack HSM or Bare Metal HSM solutions, the following PCI DSS 4.0 requirements are in scope for Google. Specific responsibilities are outlined in *Table 1: Google PCI DSS Standard Responsibilities Summary for Bare Metal Rack HSM and Bare Metal HSM*:

- **Requirement 9.1:** Processes and mechanisms for restricting physical access to cardholder data are defined and understood.

- **Requirement 9.2:** Physical access controls manage entry into facilities and systems containing cardholder data.
- **Requirement 9.3:** Physical access for personnel and visitors is authorized and managed.
- **Requirement 9.4:** Media with cardholder data is securely stored, accessed, distributed, and destroyed.

PCI DSS Additional Considerations

The following are best practice considerations for the customer to help maintain PCI DSS compliance when implementing the Google HSM solutions:

- **Network Segmentation:** The customer should ensure they have segmented their portion of the network in the Google PCI DSS cloud environment to separate networks with cardholder data from those without cardholder data. If a network is not segmented, the entire network is in scope for meeting PCI DSS, which means every component of the network must be hardened in line with the strict requirements of PCI DSS. Segmentation can be achieved through stateful firewall technologies (such as Google Firewall or Google Cloud Armor), Virtual LAN (VLAN), or VPC Service Controls. Segmentation may also be achieved through the implementation of mature zero-trust tools, such as BeyondCorp, with confirmed device- and service-level access controls.

  If a traditional perimeter security model network is implemented, the customer may define their cardholder data environment as one or more VPCs within the Google PCI DSS cloud environment (or, for hybrid or multi-cloud implementations, traditional network segments connected there to). All layers of the infrastructure that could provide an entry point to any portion of the cardholder data environment (or connections between CDE VPCs) must be considered when implementing segmentation controls.

  If a zero-trust model is implemented, each system or service within the customer's cardholder data environment may be considered as its own segmented network (i.e., microsegmentation). For simplicity, this document will refer to network segmentation, which can be understood to apply to either architecture at its respective trust boundary.

- **Access Controls:** The customer is responsible for all logical access to their HSM. The customer should ensure the access controls for the Google PCI DSS Cloud environment mirror those used for PCI DSS compliance for the rest of the customer cardholder data environment outside the Google PCI DSS cloud environment, which includes no group or shared user IDs, passwords that meet or exceed minimum levels of complexity. All access to card data and system components should be logged, with automated mechanisms implemented for performing log reviews. User access levels should be based on least privilege, assigned based on business justification, and periodically reviewed. Multi-factor authentication should be utilized for any access into the cardholder data environment. These include several controls within PCI DSS Requirements 7 and 8.
- **Secure Card Data Storage:** The network segment in the Google PCI DSS environment from where the HSMs are accessed is considered part of the customer's cardholder data environment. As a result, the customer must follow PCI DSS Requirement 3 for encryption and storage of cardholder data. This includes following the same key management best practices for encrypting and storing card data in the customer environment outside the Google PCI DSS cloud environment.
- **Secure Transmission of Card Data:** Any cardholder data transmitted from the customer environment to their Google PCI DSS cloud environment should be via a private connection, such as a direct network connection, or, if over a public network such as the Internet, via transport layer security (TLS) v1.2 at a minimum, per PCI DSS Requirement 4.

- **Vulnerability Management:** PCI DSS Requirement 5 calls for all systems within the cardholder data environment to be protected with up-to-date antivirus or anti-malware software, which would include the segment of the Google PCI DSS cloud environment from where the HSM is accessed. Based on the operating systems in use within the environment, supported anti-virus or ani-malware solutions that can meet the PCI DSS requirements can be utilized .
- **Systems and Application Environment:** The development and test environments should be separated from production environments, and access controls should be implemented to enforce the separation. In addition, organizations should consider implementing separation of duties for their security functions so that security or audit functions are separate from operations functions.
- **Monitoring and Logging:** Organizations should utilize tools for actively monitoring and inspecting the web traffic and activity to detect anomalies and reduce the risk of any compromises in the cardholder data environment.
- **Device Access Security Procedures:** For Google Bare Metal Rack HSM customers, controls for physical security of HSMs and other customer-owned equipment are a shared responsibility. Google has been assessed as meeting these controls for access to its controlled production space, and the customer must likewise ensure that any customer access to its dedicated racks complies with PCI DSS physical security requirements:
    - All access, either by customer employees or customer vendors, should be authorized, restricted based on job function, with documented approval.
    - All access, either by customer employees or customer vendors, should be monitored while on site, including logging access to each dedicated rack.
    - Customer must maintain written policies and procedures governing onsite physical access.

Note: Google is fully responsible for these controls for Google Bare Metal HSM, as customers are not allowed physical access to its production environments.

- **Device Inventory:** Customer should maintain a documented inventory of all customer-owned system components including HSMs hosted with Google (and for Bare Metal Rack HSM customers, any additional customer-owned devices placed into its dedicated racks). The list must be kept current, and include the following and should be updated when any devices are added, relocated, decommissioned, or replaced:
    - Make and model of each device.
    - Location of the device (address of facility, location, or third-party company name and location).
    - Serial number of the device or other unique identification.
    - FIPS or PTS HSM certificate approval number (if applicable)
    - Follow the key management processes and procedures as outlined within the HSM security policy guidance documents to ensure that the requirements of industry standards, such as National Institute of Standard and Technology (NIST), are met.
- **Cryptosystem Documentation:** Customers should maintain documentation of their cryptosystem, including key management procedures for keys used to provide encryption of PAN in transit or at rest, as well as inventory of all such algorithms, certificates, cipher suites and protocols.

- **Device Inventory:** Customers should maintain a list of all hardware and review it annually, including analysis of security and compliance status of the devices. HSMs which have lapsed or revoked FIPS status, for instance, may need to be identified and replaced following documented decommissioning processes.

For more information on PCI DSS compliance in Google Cloud, and how all remaining PCI DSS security requirements may apply to GCP services, customers should consult the Google PCI DSS Compliance resource.

PCI 3DS Core Security Compliance

The PCI DSS and PCI 3DS Core Security Standard are independent standards and are therefore assessed separately. A 3DE may be combined as part of the PCI cardholder data environment, or may be a completely separate standalone environment, as shown in Figure 1. 3-Domain Secure (3DS) is defined as part of the Europay, Mastercard, and Visa (EMV) 3DS Protocol and Core Functions Specification, which is managed and maintained by EMVCo. The payment brands identify if an entity is required to comply with 3DS Core Security Standard requirements, PCI DSS, or both. The PCI 3DS Core Security Standard applies to environments where 3DS Access Control Server (ACS), Director Server (DS), or 3DS Server (3DSS) functions are performed.

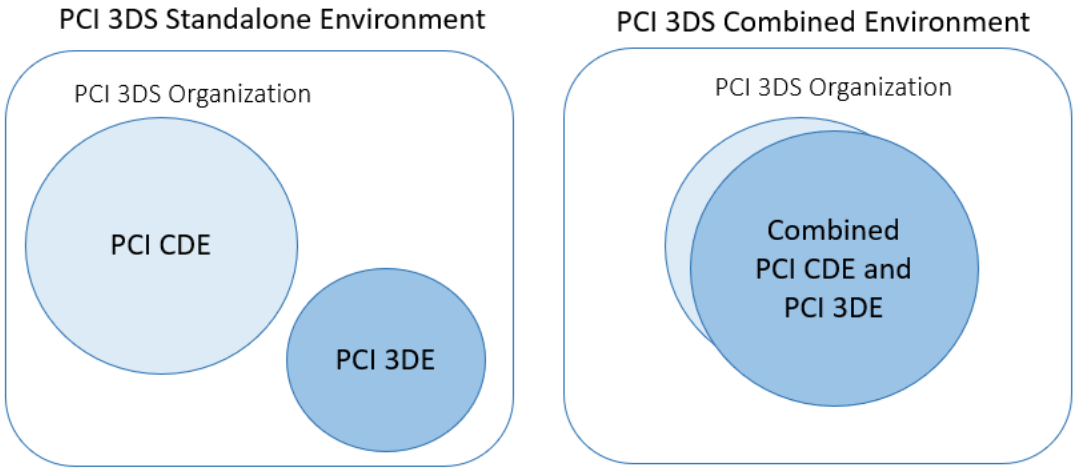

Figure 1: PCI 3DE Deployment Scenarios

As with PCI DSS requirements for the physical security of cardholder data environments, the PCI 3DS Core Security Standard shares many of the requirements for physical security for the 3DE, found in PCI 3DS Part 1. In addition, the PCI 3DS Core Security Standard has its own unique requirements for physical security in Part 2, including those specific to the physical security of HSMs, as well as system components involved in performing or facilitating 3DS transactions and system components supporting the 3DE.

For use of HSMs, the 3DS Core Security Standard contains HSM-specific requirements applicable to providers of ACS and DS components, for protection of 3DS sensitive data and cryptographic keys during transmission and storage. Such keys are required to be generated and managed in an HSM as specified in the PCI 3DS Core Security Standard, section P2.6 for PCI 3DS ACS and DS environments. As with the particular PCI DSS requirements for physical security in scope for Google customer-owned HSM

solutions, only the PCI 3DS Core Security Standard requirements related to physical security of the HSM device and information security policies are in scope for Google.

Coalfire has conducted an independent assessment of GCP as a third-party service provider for PCI 3DS. Customers using GCP for all or part of their PCI 3DS environment (3DE) and/or 3DS processes may request a copy of the GCP PCI 3DS Attestation of Compliance (AOC) and Responsibility Summary, which detail Google's compliance to applicable controls as a third-party service provider.

If the customer is using Google to host its physical HSM using Google Bare Metal Rack HSM or Bare Metal HSM solutions, the following 3DS Core Security Standard 1.0 requirements are in scope for Google. Specific responsibilities are outlined in *Table 2: Google PCI 3DS Core 1.0 Security Standard Responsibilities Summary for Bare Metal Rack HSM and Bare Metal HSM*:

- **Requirement P2-6.3:** Secure physical access to HSMs (For ACS and DS only).
- **Requirement P2-7.1:** Data center security.
- **Requirement P2-7.2:** CCTV.

For more information on 3DS data elements subject to PCI 3DS Core Security Standard, refer to the PCI 3DS Data Matrix in the References section.

PCI 3DS Core Security Additional Considerations

Customers using Google's customer-owned HSM solutions for 3DS ACS or DS services must comply with the below physical and logical security requirements for HSMs within the PCI 3DS Core Security Standard. (Security controls for any HSMs or 3DS systems hosted or managed outside of Google customer-owned HSM solutions would be the customer's full responsibility.)

- HSMs should be stored in secure area throughout their lifecycle: Customers may take delivery of HSMs for configuration and key management prior to shipment to Google for placement into production, but should ensure these devices are stored only in dedicated areas and accessible only to authorized personnel. Any physical access or logical access to the HSMs should be performed only under dual-control, to protect the integrity of the devices, configurations, and keys.
- Any personnel with logical access to HSMs should either be at the HSM console (available only for Bare Metal Rack HSM customers), or use an HSM non-console access solution that meets either one of the following approaches:
  - In version 1.0 of the 3DS Core Security Standard, requirement P2-6.2 stipulates non-console access only through the use of an HSM management solution evaluated by an independent laboratory for logical and physical security controls found in ISO 13491. In addition, devices and authentication tokens for non-console access to the HSM must be physically secured when not in use, and such access must require multi-factor authentication (MFA), be cryptographically authenticated, and performed under dual control only by authorized personnel. All non-console activity must be monitored and originate only from a segmented network within the 3DE. Using this method, clear-text keys may not be loaded or exported from the HSM.

  or

  - In September 2023, an alternate set of requirements for P2-6.2 was published in the PCI 3DS Core v1.x Technical FAQs, supporting non-console access using a FIPS 140-2 / 140-3 Level 3+ or PCI PTS-listed SCD over a secure channel from outside the 3DE. Such connections must also enforce MFA, and be performed under split knowledge and

dual control. All remote key loading using this method must use a designated key transport key exchanged between the SCD and the HSM.

- For Bare Metal Rack HSM customers, physical access to HSMs or other 3DS systems within the dedicated rack must be restricted based on job function and performed only under dual control, including the installation and decommissioning of HSM devices.

All 3DS customers whose solution relies partially or entirely on GCP services must identify the accurate scope of their 3DS environment and applicable controls.

Recommendations noted for PCI DSS in this document should also be applied for PCI 3DE, since the customer's 3DE must reside within a compliant PCI DSS CDE, or meet all controls in 3DS Core Part 1. Customers using the customer-owned HSM solutions are responsible for all logical security controls for HSMs. Customers are also responsible for physical access security for all other 3DE systems not housed within Google GCP.

The following additional controls should be considered for any 3DE hosted within the GCP environment:

- **Network Segmentation:** 3DS can be part of the PCI DSS environment or can be hosted separately. Based on the deployment scenario, the segmentation controls, such as the use of firewalls and VLAN or ACLs, can be implemented for segmenting out-of-scope networks.
- **Boundaries Protection:** Traffic between various PCI 3DS components should be restricted and permitted only via approved interfaces.
- **Availability Mechanisms:** To maintain integrity of the PCI 3DE, it should be architected with high availability as a key factor while designing infrastructure, systems, or software. To qualify for a 99.99% uptime SLA, customers must deploy HSMs in a minimum of two Google Cloud Regions and deploy a minimum of four HSMs per region (at least two HSMs per rack in at least two racks).
- **Logical Access:** Strong authentication techniques and approved interfaces should be used for providing access to third-party entities that need to connect to the 3DE.
- **Secure Virtual Private Network (VPN):** Any access to 3DE using VPNs should be configured to provide strong security communications (e.g., using trusted Certificate Authority [CA]).

For details on how all remaining 3DS Core security requirements may apply to GCP services that support the 3DE, customers should consult the Google 3DS AOC and Shared Responsibility Summary.

PCI P2PE Compliance

The PCI P2PE standard has its own unique requirements for the physical security of devices handling the encryption or decryption of account data, including cryptographic key management activities. The PCI P2PE program was developed to standardize protection for encryption that can simplify compliance for PCI DSS merchants. The PCI P2PE program does not replace PCI DSS but offers eligible merchants an effective option for removing certain network assets from scope and reducing the number of applicable controls for the remaining environment. The standards eligibility criteria, including physical security requirements, for PCI P2PE solution providers or PCI P2PE component providers are detailed within the PCI P2PE 3.1 standard.

If a customer is using one of the Google customer-owned HSM solutions as part of is P2PE offering, the following PCI P2PE requirements may be deemed in scope for Google, and suitable for validation as part of the entity's assessment. Please note that unique P2PE program requirements prevent Google from performing an independent assessment against these controls. Specific responsibilities are outlined in

Table 3: Google PCI P2PE Standard Responsibilities Summary for Bare Metal Rack HSM and Bare Metal HSM:

- **Requirement 4B-1.5:** Inspections of decryption HSMs by authorized personnel must be performed at least quarterly to detect tampering or modification of devices. These inspections are performed at the request of the customer, so it ultimately falls to the customer to request and maintain records of these HSM inspections. Alternatively, Google Bare Metal Rack HSM customers may choose to coordinate scheduled visits to perform these onsite device inspections directly.
- **Requirement 4C-1.2:** Mechanisms must be implemented to detect and respond to suspicious activity.
- **Requirement 29-1:** HSMs must be placed into service only if there is assurance that the equipment has not been subjected to unauthorized modifications, substitution, or tampering and has not otherwise been subject to misuse prior to deployment.
- **Requirement 29-4:** Dual-control mechanisms must exist to prevent substitution or tampering of HSMs – both deployed and spare or backup devices – throughout their lifecycle.
- **Requirement 29-4.1:** HSM serial numbers must be compared to the serial numbers documented by the sender (sent using a different communication channel from the device) to ensure device substitution has not occurred. A record of device serial-number verification must be maintained.
- **Requirement 29-4.4:** Inspect and test all HSMs – either new or retrieved from secure storage – prior to installation to verify devices have not been tampered with or compromised.
- **Requirement 29-5:** Maintain HSMs in tamper-evident packaging or in secure storage until ready for installation.
- **Requirement 31-1:** Procedures must be in place to ensure that any HSMs to be removed from service—e.g., retired or returned for repair—are not intercepted or used in an unauthorized manner, including rendering all secret and private keys, key material, and account data stored within the device irrecoverable.

Unlike PCI DSS, PCI 3DS and PCI PIN, where Google can provide an attestation of compliance (AOC) demonstrating that applicable controls have already been independently assessed by a credentialed assessor, the PCI P2PE program does not allow partial assessments of third-party service providers except where they are eligible as component providers. There is currently no component provider type related to the services that Google providers. In such cases, PCI FAQ 1369 confirms that providers may provide evidence to the customer's P2PE Assessor to demonstrate where they are meeting P2PE requirements on behalf of the customer. Customers should contact their Google account executive for assistance with audit support of this nature.

PCI P2PE Additional Considerations

The P2PE solution providers or component providers must comply with the below physical and logical security requirements for decryption HSMs subject to the PCI P2PE standard. (HSMs hosted and managed by customers in their own facility that are not part of the Google customer-owned HSM solutions would be the customer's responsibility and must also comply with below requirements.) Recommendations noted for PCI DSS should also be applied to the PCI P2PE environment.

- Documented policies should be in place for commissioning and decommissioning customer-supplied HSMs, to ensure that they are being handled in accordance with PCI P2PE requirements for physical handling of HSMs.

- All physical access to the HSMs by customers during commissioning (prior to shipment to Google facilities) and decommissioning (after receipt from Google for repair or replacement, if applicable), should require dual control and be logged. Similarly, for Bare Metal Rack HSM customers, it is the customer's responsibility to ensure that customer physical access to HSMs within Google facilities is also performed under dual control and logged.
- Procedures should be in place for quarterly inspection of the HSMs to detect device tampering, either directly (for Google Bare Metal Rack HSM customers) or indirectly by initiating a request for inspection of customer-owned HSMs.
- An inventory of all HSMs with model names and serial numbers should be maintained and updated as devices are received from the HSM provider, delivered to Google for installation, removed from service, and ultimately sent back to the customer or destroyed. All HSMs received from customers should be in tamper-proof packaging with instructions that they remain in packaging until installation.
- The P2PE decryption environment is required to be housed within a PCI DSS cardholder data environment as a combined environment, as shown in Figure 2. The P2PE customer is responsible for performing a QSA-led Report on Compliance (ROC) annually of this environment, but may leverage Google's PCI DSS ROC to aid in meeting applicable controls.

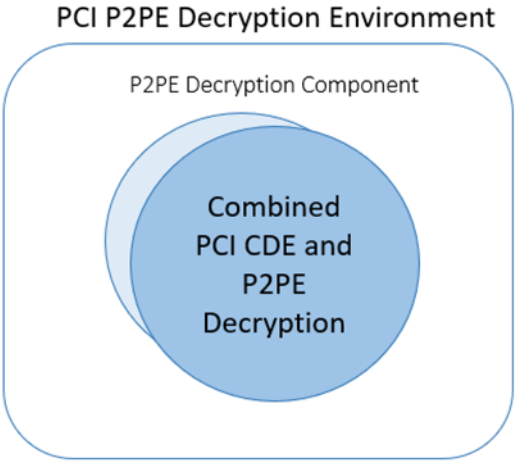

Figure 2: PCI P2PE Decryption Environment Deployment Scenario

- HSMs used for P2PE decryption should be on an isolated and dedicated network segment (VPC), as identified in Figure 3. The network should be dedicated solely for decryption operations or transaction processing.

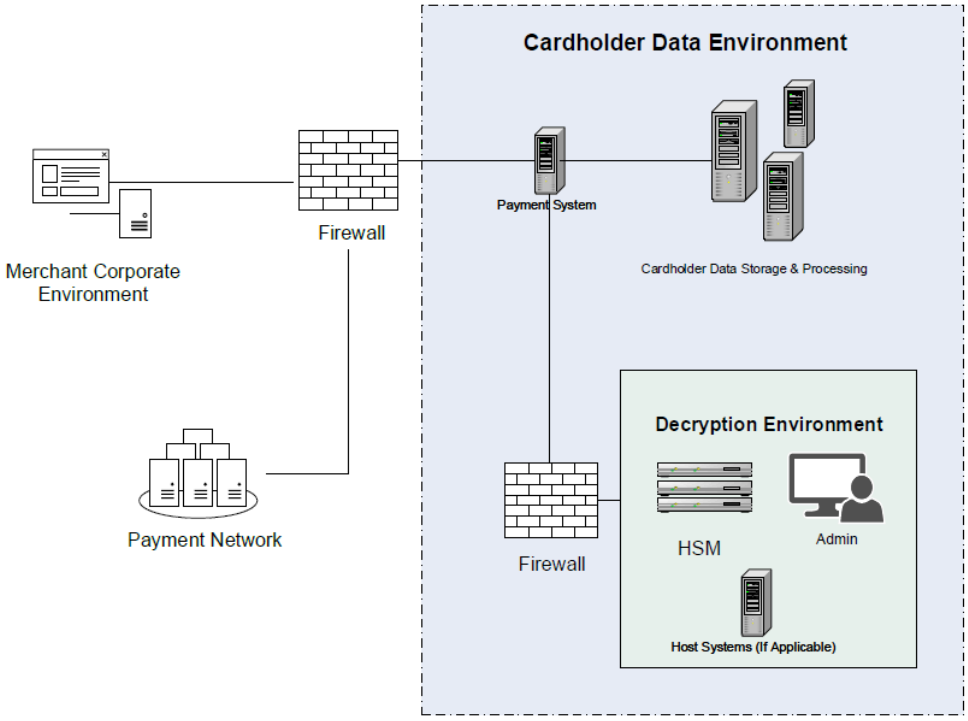

Figure 3: Segmented Decryption Environment within PCI DSS CDE

PCI PIN Compliance

The PCI PIN standard has its own unique requirements for the physical security of devices handling the encryption or decryption of PIN data, including cryptographic key management activities. The PCI PIN program was developed to standardize protection for encryption of PIN that can protect payments from fraudulent use. The PCI PIN security standard covers secure management, processing, and transmission of PIN data during online and offline payment card transaction processing. The PCI PIN standard applies to acquiring institutions and agents and those entities responsible for PIN transaction processing of PCI brand cards, or any entity as directed by a participating payment brand. The eligibility criteria, including physical security requirements, for PCI PIN are identified within the PCI PIN 3.1 security requirements.

Coalfire has conducted an independent assessment of GCP as a third-party service provider for PCI PIN. Customers using GCP for all or part of their PCI PIN environment and/or processes may request a copy of the GCP PCI PIN Attestation of Compliance (AOC) and Responsibility Summary, which detail Google's compliance to applicable controls as a third-party service provider.

If a customer is using one of the Google customer-owned HSM solutions as part of its PCI PIN offering, the following PCI PIN requirements may be in scope for Google. Specific responsibilities are outlined in *Table 4: Google PCI PIN Standard Responsibilities Summary for Bare Metal Rack HSM and Bare Metal HSM*:

- **Requirement 29-1:** HSMs must be placed into service only if there is assurance that the equipment has not been subject to unauthorized modification, substitution, or tampering and has not otherwise been subject to misuse prior to deployment.
- **Requirement 29-4:** Dual-control mechanisms must exist to prevent substitution or tampering of HSMs – both deployed and spare or backup devices – throughout their lifecycle.
- **Requirement 29-4.1:** HSM serial numbers must be compared to the serial numbers documented by the sender (sent using a different communication channel from the device) to ensure device substitution has not occurred. A record of device serial-number verification must be maintained.
- **Requirement 29-4.4:** Inspect and test all HSMs – either new or retrieved from secure storage – prior to installation to verify devices have not been tampered with or compromised.
- **Requirement 29-5:** Maintain HSMs in tamper-evident packaging or in secure storage until ready for installation.
- **Requirement 31-1:** Procedures must be in place to ensure that any HSMs to be removed from service—e.g., retired or returned for repair—are not intercepted or used in an unauthorized manner, including rendering all secret and private keys, key material, and account data stored within the device irrecoverable.

PCI PIN Additional Considerations

Entities eligible for PIN validation must comply with the below physical and logical security requirements for HSMs subject to the PCI PIN standard for PIN transaction processing. (HSMs hosted and managed by customers in their own facility that are not part of the Google customer-owned HSM solutions would be the customer's responsibility and must also comply with below requirements.) Recommendations noted for PCI DSS should also be applied to the PCI PIN environment.

- Documented policies should be in place for commissioning and decommissioning customer supplied HSMs to ensure that they are being handled in accordance with PCI PIN requirements for physical handling of HSMs.

- All physical access to the HSMs by customers during commissioning and decommissioning, should require dual control and be logged. This also applies to Bare Metal Rack HSM customers who require physical access to HSMs within Google facilities for physical maintenance.
- An inventory of all HSMs with model names and serial numbers should be maintained and updated as devices are received from the customer, removed, and sent back to the customer, or destroyed. All HSMs received from customers should be in tamper-proof packaging and remain packaged until installation.

Methodology

Coalfire completed a detailed technical assessment of the Google customer-owned HSM solutions from November 28, 2023, to May 14, 2024, using industry and audit best practices. Coalfire conducted a virtual walkthrough of the provider facility used by the solution.

At a high level, testing consisted of the following tasks:

1. Analysis of the architecture, configuration, and procedures for Google Bare Metal Rack HSM and Bare Metal HSM solutions.
2. Review of technical documentation, including policy and procedures for the customer-owned HSM solutions as well as the Google-managed facility access procedures.
3. Onsite and remote visits to Google datacenter facilities, to directly observe physical access controls and implementation of security measures.
4. Interview of support personnel both during and separately from the datacenter walkthroughs, to confirm the functionality of the solution and discuss details for controls within the standards.

Google CUSTOMER-Owned HSM Solution Architecture

Below is a sample dual region topology architecture that demonstrates the customer network and connectivity to Google when it is hosting customer HSMs.

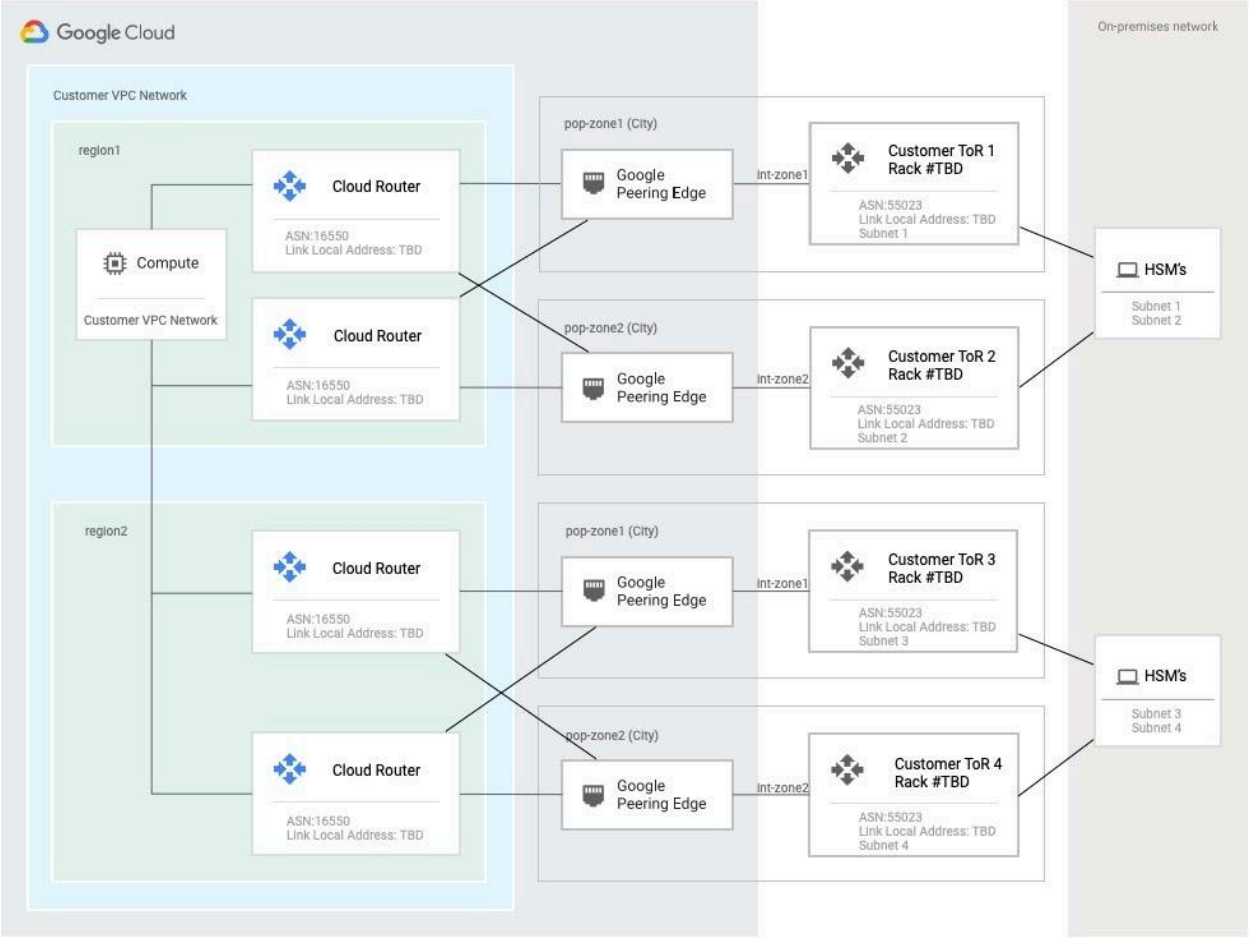

Figure 4: Google Customer-Owned HSM Network Topology Architecture (single rack)

The operational elements of the Google customer-owned HSM solutions are discussed below:

- **Contracts Agreement with Customer:** The service provided by the Google HSM Solution is restricted to only the physical handling of the HSM by Google at and within the designated production facilities. Google has no logical access to the HSM at any time during its lifecycle.
- **Commissioning Process:** Customers are provided specific instructions on the environment so that they can prepare the shipment of the HSM to the Google provider facility. Google staff receive the device shipped to the provider facility and maintain an inventory of devices they receive and deploy.
- **Google Device Handling and Setup Process:** Google staff mounts the HSM within the shared (or, in the case of Google Bare Metal Rack HSM service, dedicated) rack space in the provider facility and connect power and network cabling. In addition, the facility staff coordinate to pre-configure the rack, top-of-rack switches, and connectivity, providing a redundant power supply and a network routing required for each rack. Google provides a racking service for the customer's devices and

validates connectivity with the customer. Google approves all instructions for HSM installation with the Google customer prior to providing them to the Google staff at the facility location.

- **Maintenance:** Google may perform remote hands services that include activities such as power cycling and reboot; pushing and resetting of toggle switches, buttons, or external physical settings; visual observations and reports for environmental status, display lights and terminal display information; device renaming and labeling using external configuration capabilities; re-cabling, labeling, or cable management (ties/bundling); audits and reporting (asset management, service tag information, and rack elevation plan); and other activities upon customer request which, at Google's sole discretion, do not require logical or console access to the HSM device.
- **Customer Remote Management of Device:** Google mounts the device in the provider facility, and all logical access and management of the HSM is handled only by the customer.
- **Decommissioning Process:** The colocation provider staff performs remote hands services and other activities upon customer request. If the device needs to be decommissioned, the Google staff can remove the network cables, unplug the device from the power source, and remove it from the rack. Staff can then ship the device back to the customer per the customer's instructions. If the device cannot be securely packaged and returned, the staff will destroy the device according to secure destruction procedures.

Results Summary

The following are relevant highlights from this assessment for compliance with each of the four standards for the Google HSM solutions:

1. The Google customer-owned HSM solutions have controls in place for complying with the applicable PCI DSS requirements listed below. In addition, the provider facility used by Google undergo their own PCI DSS assessments that cover the following applicable requirements:
    a. The provider facility hosting the solution has sufficient entry controls to limit and monitor physical access to the HSMs installed in their environment.
    b. Procedures are in place to easily distinguish between onsite personnel and visitors.
    c. Physical access for onsite personnel to sensitive areas is controlled.
    d. Procedures are implemented to identify and authorize visitors, including visitor logs and closed-circuit television (CCTV) monitors.
2. The Google customer-owned HSM solutions have controls in place for complying with the following applicable PCI 3DS Core Security Standard requirements on behalf of their customers:
    a. The facility hosting the solution provides adequate physical security to limit access to the HSMs installed in the facility.
    b. The facility provides physical security for hosted HSMs that meets the requirements of the standard.
3. The Google customer-owned HSM solutions has controls in place for complying with the following applicable PCI P2PE requirements on behalf of their customers:
    a. The facilities hosting the solution have intrusion detection systems (IDS) that provide continuous (i.e., 24/7) monitoring of the facilities.

b. The facility maintains an inventory of all HSM devices received and installed, including a list of device model names and serial numbers.

c. The facility has policies and procedures in place for verifying the secure shipment of HSMs to and from the facility location, including verifying that devices have not been tampered with during shipment.

4. Procedures are in place that require the dual control of HSMs for the initial commissioning process at the facility location. Once mounted within the rack, strict procedural controls and monitoring prevent access to customer equipment except when authorized as part of a process managed under dual control. Customers are responsible for managing dual control access for other lifecycle phases of HSM, and are encouraged to perform the initial commissioning on their own premises, then put the HSM into transport mode and ship it to the Google facility.

Assessor Comments

Coalfire's assessment scope focused on confirming that the controls implemented at the Google-managed facility for its Google customer-owned HSM solutions meet PCI DSS, PCI 3DS Core Security Standard, PCI P2PE, and PCI PIN physical security requirements on behalf of its customers.

It is important to note that any solution as detailed in this white paper does not alleviate a customer's responsibility to meet applicable standard assessment and compliance requirements.

For PCI DSS compliance, be advised that disregarding PCI DSS requirements and security best practice controls for systems and networks both within and outside of PCI DSS scope can introduce many other security or business continuity risks to the merchant. Security and business risk mitigation should be any organization's goal and focus for selecting security controls.

The PCI 3DS Core Security, PCI P2PE, and PCI PIN standards should be assessed for eligibility, and a risk management approach should be followed to meet controls within those standards.

Note that Google's role in the deployment of the Google customer-owned HSM solutions is limited to the physical installation of the customer provided HSM hardware in the provider facility. Google has no logical access to HSMs at any point in the devices' lifecycle.

Appendix A: Responsibility Matrices

PCI DSS Responsibilities

The below is a breakdown of the specific PCI DSS requirements in scope for physical security and the respective responsibilities of both Google and a customer using the Google customer-owned HSM solutions. The following are a subset of the PCI DSS requirements that pertain to the physical security of the HSM within Google facilities. The remaining requirements are not in scope for this review and, as a result, are not included.

It is the customer's responsibility to identify in-scope controls, processes, systems, networks, applications, and third-party service providers. The customer should obtain the latest Google PCI DSS AOC and Responsibility Summary for evidence of Google's responsibilities related to the HSM solutions, as detailed below, as well as any other Google services in scope for PCI DSS.

PCI DSS 4.0 REQUIREMENT	Google Responsibility	Customer Responsibility
9.1.1 All security policies and operational procedures that are identified in Requirement 9 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	Google maintains documented policies and procedures that apply to its employees and agents for physical security within Google production facilities. Coalfire reviewed security policies and training records and confirmed that all physical security policies are up to date and made known to applicable parties.	Customers are responsible for ensuring that its policies and procedures are documented and known to all affected parties. For Google Bare Metal Rack HSM customers, this should include maintenance of policies and procedures applicable to physical access to customer HSMs in Google facilities.
9.1.2 Roles and responsibilities for performing activities in Requirement 9 are documented, assigned, and understood.	Google has documented and assigned roles and responsibilities for applicable activities by Google personnel. Roles and responsibilities are understood by assigned individuals. Coalfire observed through onsite and virtual walkthrough and interview with product and facility staff that roles and responsibilities are documented and well understood.	Customers are responsible for documenting and assigning roles and responsibilities for applicable activities. For Google Bare Metal Rack HSM customers, this should include roles and responsibilities for personnel authorized to physically access customer HSMs in Google facilities. Roles and responsibilities must be understood by assigned individuals.
9.2.1 Appropriate facility entry controls are in place to restrict physical access to systems in the CDE.	Google maintains the physical security controls for all facilities that host GCP Products. Coalfire reviewed policies and procedures and observed a virtual and onsite walkthroughs of production facilities and confirmed that the control is in place.	Where requirement 9.2 and its sub-requirements apply to facility security controls for facilities that host GCP products, these controls are not applicable for the customer. For Google Bare Metal Rack HSM customers, access to the production facility will be subject to Google's physical access controls. Customer onsite activities are thus subject to

PCI DSS 4.0 REQUIREMENT	Google Responsibility	Customer Responsibility
		compliance with these controls, and must not supplant Google's these physical security controls.
9.2.1.1 Individual physical access to sensitive areas within the CDE is monitored with either video cameras or physical access control mechanisms (or both) as follows: • Entry and exit points to/from sensitive areas within the CDE are monitored. • Monitoring devices or mechanisms are protected from tampering or disabling. • Collected data is reviewed and correlated with other entries. • Collected data is stored for at least three months, unless otherwise restricted by law.	Google maintains the physical security controls for all facilities that host GCP Products. Coalfire observed during virtual and physical walkthroughs at GCP facilities that badge access with unique PIN or biometric authentication ensures single-entry, positive authenticated access to a single person to enter the designated area.	Where requirement 9.2 and its sub-requirements apply to facility security controls for facilities that host GCP products, these controls are not applicable for the customer.
9.2.2 Physical and/or logical controls are implemented to restrict use of publicly accessible network jacks within the facility.	Google maintains the physical security controls for all facilities that host GCP Products. Coalfire observed during onsite and virtual walkthroughs of GCP facilities that there were no jacks in public areas.	Where requirement 9.2 and its sub-requirements apply to facility security controls for facilities that host GCP products, these controls are not applicable for the customer.
9.2.3 Physical access to wireless access points, gateways, networking/ communications hardware, and telecommunication lines within the facility is restricted.	Google maintains the physical security controls for all facilities that host GCP Products. Coalfire observed during onsite and virtual walkthroughs of GCP facilities that there no accessible wireless networking or telecommunication lines outside of restricted areas.	Where requirement 9.2 and its sub-requirements apply to facility security controls for facilities that host GCP products, these controls are not applicable for the customer.
9.2.4 Access to consoles in sensitive areas is restricted via locking when not in use.	Google maintains the physical security controls for all facilities that host GCP Products. Coalfire reviewed policies and procedures and performed onsite and virtual walkthroughs of facilities and observed that all sensitive areas are accessible only by authorized personnel, and require badge with PIN and/or biometric for access.	Where requirement 9.2 and its sub-requirements apply to facility security controls for facilities that host GCP products, these controls are not applicable for the customer.

PCI DSS 4.0 REQUIREMENT	Google Responsibility	Customer Responsibility
9.3.1 Procedures are implemented for authorizing and managing physical access of personnel to the CDE, including: • Identifying personnel. • Managing changes to an individual's physical access requirements. • Revoking or terminating personnel identification. • Limiting access to the identification process or system to authorized personnel.	Google maintains the physical security controls for all facilities that host GCP Products. Coalfire reviewed policies and procedures and verified through observation during onsite and virtual walkthroughs that the control is in place.	Where requirement 9.3 and its sub-requirements apply to authorization of personnel for access to facilities that host GCP products, these controls are not applicable for the customer. For Google Bare Metal Rack HSM customers, the customer is responsible to coordinate onsite activities, including identification of authorized personnel for each visit, and informing Google where such access may be limited or revoked.
9.3.1.1 Physical access to sensitive areas within the CDE for personnel is controlled as follows: • Access is authorized and based on individual job function. • Access is revoked immediately upon termination. • All physical access mechanisms, such as keys, access cards, etc., are returned or disabled upon termination.	Google maintains the physical security controls for all facilities that host GCP Products. Coalfire reviewed policies and procedures and verified through observation during onsite and virtual walkthroughs that the control is in place.	Where requirement 9.3 and its sub-requirements apply to authorization of personnel for access to facilities that host GCP products, these controls are not applicable for the customer.
9.3.2 Procedures are implemented for authorizing and managing visitor access to the CDE, including: • Visitors are authorized before entering. • Visitors are escorted at all times. • Visitors are clearly identified and given a badge or other identification that expires. • Visitor badges or other identification visibly distinguishes visitors from personnel.	Google maintains the physical security controls for all facilities that host GCP Products. Coalfire reviewed policies and procedures, review of documented access requirements, samples of access badges and verification during onsite and virtual walkthroughs that visitors are authorized, identified, escorted, that Google badges visibly distinguish visitors.	Where requirement 9.3 and its sub-requirements apply to authorization of personnel for access to facilities that host GCP products, these controls are not applicable for the customer.
9.3.3 Visitor badges or identification are surrendered or deactivated before visitors leave the facility or at the date of expiration.	Google maintains the physical security controls for all facilities that host GCP Products. Coalfire observed during onsite walkthrough of production facilities that visitors' badges must be surrendered before leaving, and reviewed records confirming access is revoked.	Where requirement 9.3 and its sub-requirements apply to authorization of personnel for access to facilities that host GCP products, these controls are not applicable for the customer.
9.3.4 A visitor log is used to maintain a physical record of visitor activity within	Google maintains the physical security controls for all facilities that host GCP Products.	Where requirement 9.3 and its sub-requirements apply to authorization of personnel for access

PCI DSS 4.0 REQUIREMENT	Google Responsibility	Customer Responsibility
the facility and within sensitive areas, including: • The visitor's name and the organization represented. • The date and time of the visit. • The name of the personnel authorizing physical access. • Retaining the log for at least three months, unless otherwise restricted by law.	Coalfire reviewed visitor access records and confirmed that all required information is maintained for all visitors.	to facilities that host GCP products, these controls are not applicable for the customer.
9.4.1 All media with cardholder data is physically secured.	Google maintains the physical security and media handling controls for data centers and colocation facilities that host GCP Products. Google does not store customer data on removable media.	Customers are responsible for backup, compliance, and destruction of any media containing cardholder data outside of the GCP environment.
9.4.1.1 Offline media backups with cardholder data are stored in a secure location.	Google maintains the physical security and media handling controls for data centers and colocation facilities that host GCP Products. Media related to customer-owned HSMs is subject to these controls, but is never accessed or stored by Google.	Customers are responsible for backup, compliance, and destruction of any media containing cardholder data outside of the GCP environment.
9.4.1.2 The security of the offline media backup location(s) with cardholder data is reviewed at least once every 12 months.	Google maintains the physical security and media handling controls for data centers and colocation facilities that host GCP Products. Media related to customer-owned HSMs is subject to these controls, but is never accessed or stored by Google.	Customers are responsible for backup, compliance, and destruction of any media containing cardholder data outside of the GCP environment.
9.4.2 All media with cardholder data is classified in accordance with the sensitivity of the data.	Google maintains the physical security and media handling controls for data centers and colocation facilities that host GCP Products. Media related to customer-owned HSMs is subject to these controls, but is never accessed or stored by Google.	Customers are responsible for backup, compliance, and destruction of any media containing cardholder data outside of the GCP environment.
9.4.3 Media with cardholder data sent outside the facility is secured as follows: • Media sent outside the facility is logged. • Media is sent by secured courier or other delivery method that can be accurately tracked.	Google maintains the physical security and media handling controls for data centers and colocation facilities that host GCP Products. Media related to customer-owned HSMs is subject to these controls, but is never accessed or stored by Google.	Customers are responsible for backup, compliance, and destruction of any media containing cardholder data outside of the GCP environment.

PCI DSS 4.0 REQUIREMENT	Google Responsibility	Customer Responsibility
• Offsite tracking logs include details about media location.		
9.4.4 Management approves all media with cardholder data that is moved outside the facility (including when media is distributed to individuals).	Google maintains the physical security and media handling controls for data centers and colocation facilities that host GCP Products. Media related to customer-owned HSMs is subject to these controls, but is never accessed or stored by Google.	Customers are responsible for backup, compliance, and destruction of any media containing cardholder data outside of the GCP environment.
9.4.5 Inventory logs of all electronic media with cardholder data are maintained.	Google maintains the physical security and media handling controls for data centers and colocation facilities that host GCP Products. Media related to customer-owned HSMs is subject to these controls, but is never accessed or stored by Google.	Customers are responsible for backup, compliance, and destruction of any media containing cardholder data outside of the GCP environment.
9.4.5.1 Inventories of electronic media with cardholder data are conducted at least once every 12 months.	Google maintains the physical security and media handling controls for data centers and colocation facilities that host GCP Products. Media related to customer-owned HSMs is subject to these controls, but is never accessed or stored by Google.	Customers are responsible for backup, compliance, and destruction of any media containing cardholder data outside of the GCP environment.
9.4.6 Hard-copy materials with cardholder data are destroyed when no longer needed for business or legal reasons, as follows: • Materials are cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed. • Materials are stored in secure storage containers prior to destruction.	Google maintains the physical security and media handling controls for data centers and colocation facilities that host GCP Products. Media related to customer-owned HSMs is subject to these controls, but is never accessed or stored by Google.	Customers are responsible for backup, compliance, and destruction of any media containing cardholder data outside of the GCP environment.
9.4.7 Electronic media with cardholder data is destroyed when no longer needed for business or legal reasons via one of the following: • The electronic media is destroyed. • The cardholder data is rendered unrecoverable so that it cannot be reconstructed.	Google maintains the physical security and media handling controls for data centers and colocation facilities that host GCP Products. Media related to customer-owned HSMs is subject to these controls, but is never accessed or stored by Google. These controls include ensuring that any media leaving Google facilities, including customer-owned HSMs, must	Customers are responsible for backup, compliance, and destruction of any media containing cardholder data outside of the GCP environment. Customer may be responsible to work with Google to coordinate secure erasure of customer-owned HSMs during the decommissioning process.

PCI DSS 4.0 REQUIREMENT	Google Responsibility	Customer Responsibility
	have electronic media securely wiped or destroyed prior to return.	

Table 1: Google PCI DSS Standard Responsibilities Summary for Bare Metal Rack HSM and Bare Metal HSM

PCI 3DS Core Security Responsibilities

The below is a breakdown of the specific PCI 3DS Core Security Standard requirements in scope for physical security and the respective responsibilities for both Google and customers using the Google customer-owned HSM solutions. The following are a subset of the PCI 3DS Core Security Standard requirements that pertain to Google's responsibility for physical security of the customer-owned HSM within Google's facilities. Since Bare Metal Rack HSM customers may also be allowed physical access to their HSM racks, additional customer responsibilities are identified.

The remaining requirements are not in scope for this review and, as a result, were not included in this list. The remote access management of HSMs that are hosted with Google are the responsibility of the customer and all physical security controls apply for the devices used for performing the remote management of HSMs.

PCI 3DS Core Security 1.0 REQUIREMENTs	Google Responsibility	Customer ResponsIbility
P2-6.3.1: HSMs are stored in a dedicated area(s).	Google stores all HSMs for Bare Metal Rack HSM, and Bare Metal HSM in dedicated HSM racks, and leverages physical, logical, and procedural controls to prevent access to another customer's HSMs. Coalfire observed during a virtual walkthrough that racks designated for Bare Metal Rack HSM services are separate and unique racks dedicated solely to the customer. The rack and/or cage doors are also controlled by badge access and only authorized individuals can access the racks. No Google staff can perform any actions directly on the HSMs and can only handle the physical installation, rebooting and decommissioning of devices on the customer's behalf.	Customers are responsible for secure storage of HSMs throughout their lifecycle, including provisioning and decommissioning activities that take place outside GCP facilities. While hosting customer-owned HSMs within GCP facilities, the customer can rely on Google's validated compliance for evidence that HSMs storage is performed in dedicated areas.
P2-6.3.2: Physical access to the HSMs is restricted to authorized personnel and managed under dual control.	Google maintains Bare Metal HSM devices in racks specific to the Bare Metal HSM service, and maintains Bare Metal Rack HSM devices in customer-dedicated racks. Coalfire observed during onsite and virtual walkthroughs that Bare Metal Rack HSM rack and/or cage doors are controlled by badge access and only authorized individuals can access the racks. Google leverages access controls and strict work authorization procedures to restrict personnel from accessing these areas except under dual control. Only authorized Google personnel are	Bare Meta Rack HSM customers are responsible for maintaining procedures ensuring customer access to production HSMs is restricted to authorized personnel. Customers are responsible for managing physical access under dual control at the locations where HSMs are provisioned or decommissioned outside of GCP facilities.

PCI 3DS Core Security 1.0 REQUIREMENTs	Google Responsibility	Customer ResponsIbility
	allowed to perform physical installation, rebooting, and decommissioning of devices on the customer's behalf, and dual control is maintained throughout this process.	
P2-7.1.2: Data centers supporting Access Control Server (ACS) and Directory Server (DS) are equipped with a positively controlled single-entry portal (e.g., mantrap), that: • Requires positive authentication prior to granting entry; and • Grants entry to a single person for each positive authentication.	Google is responsible for all physical security controls for production GCP facilities. Coalfire observed during virtual and physical walkthroughs at GCP facilities that badge access with unique PIN or biometric authentication ensures single-entry, positive authenticated access to a single person to enter the designated area.	Customers are responsible for managing the physical security of systems not managed within the GCP environment.
P2-7.1.3: Doors to areas within the data center that contain 3DS systems are fitted with an electronic access-control system (e.g., card reader, biometric scanner) that controls and records all entry and exit activities.	Google is responsible for ensuring that access control systems are deployed to access the area where the HSMs are stored in the colocation provider location. Google also provides badge access to racks hosting customer HSMs. Coalfire observed during onsite and virtual walkthroughs that user access requires a badge access card and unique PIN or biometric to access the facility location.	Customers are responsible for managing the physical security of systems not managed within the GCP environment.
P2-7.1.4: Multi-factor authentication is required for entry to telecommunications rooms that are not located within a secure data center.	Google is responsible for all physical security controls for GCP facilities, including any secondary telecommunications rooms, if applicable. Coalfire observed in onsite and virtual walkthroughs that production facilities do not have telecommunications rooms outside of the secure data center, and that Google facilities for other secure operations require multifactor authentication.	Customers are responsible for managing the physical security of systems not managed within the GCP environment.
P2-7.1.5: Entry controls prevent piggy-backing by granting access to a single person at a time, with each person being identified and	Google is responsible for all physical security controls for production GCP facilities.	Customers are responsible for managing the physical security of systems not managed within the GCP environment.

PCI 3DS Core Security 1.0 REQUIREMENTs	Google Responsibility	Customer ResponsIbility
authenticated before access is granted.	Coalfire observed an entry through a single-entry portal that allowed only one person to enter during onsite and virtual walkthroughs of the facility location to verify that this control is in place.	
P2-7.1.6: A physical intrusion-detection system that is connected to the alarm system is in place.	Google is responsible for all physical security controls for production GCP facilities. Coalfire observed the implementation of physical IDS system, and verified that attempted unauthorized entry during onsite and virtual walkthroughs generated an audible alarm and SOC alerting, verifying that this control is in place.	Customers are responsible for managing the physical security of systems not managed within the GCP environment.
P2-7.1.7: Physical connection points leading into the 3DE are controlled at all times.	Google is responsible for all physical security controls for production GCP facilities. Coalfire observed during the onsite and virtual walkthroughs that access to the production environments is constantly controlled and monitored by dedicated security personnel.	Customers are responsible for managing the physical security of systems not managed within the GCP environment.
P2-7.2.1: CCTV cameras are located at all entrances and emergency exit points and capture identifiable images, at all times of the day and night.	Google is responsible for all physical security monitoring controls for production GCP facilities. Coalfire observed during onsite and virtual walkthroughs that CCTV cameras exist at all entrances and exit points and that identifiable CCTV recordings are captured at all times.	Customers are responsible for managing the physical security of systems not managed within the GCP environment. Customers have overall responsibility for physical security. However, for the purposes of this control, the customer can rely on Google's validated compliance for meeting the CCTV camera requirements for the Google customer-owned HSM solutions. Customers are responsible for ensuring that CCTV cameras monitoring entry and exit points exist within the 3DE hosted by the customer.

PCI 3DS Core Security 1.0 REQUIREMENTs	Google Responsibility	Customer ResponsIbility
P2-7.2.2: CCTV recordings are time stamped.	Google is responsible for all physical security monitoring controls for production GCP facilities. Coalfire observed during onsite and virtual walkthroughs that CCTV recordings confirm that timestamps are included in recordings.	Customers are responsible for managing the physical security of systems not managed within the GCP environment.

Table 2: Google PCI 3DS Core Security Standard Responsibilities Summary for Bare Metal Rack HSM and Bare Metal HSM

PCI P2PE Responsibilities

P2PE solution providers or P2PE component providers can utilize the Google Bare Metal Rack HSM and Bare Metal HSM solutions to help meet HSM needs and provide physical security for the customer-owned HSM solutions hosted within Google cloud environment. The remote access management of HSMs that are hosted in the Google cloud environment are the responsibility of the customer and all physical security controls apply for the devices used to perform remote management of HSMs.

The below is a breakdown of the specific PCI P2PE requirements in scope for physical security and the respective responsibilities for both Google and its customer using the Google customer-owned HSM solutions:

PCI P2PE REQUIREMENT	Google Responsibility	Customer ResponsIbility
4B-1.5: Inspections of decryption devices by authorized personnel must be performed at least quarterly to detect tampering or modification of devices. Inspections to include: • The device itself • Cabling/connection points • Physically connected devices	Google is responsible for all physical security controls for production GCP facilities. Coalfire observed through interviews with staff that inspection of customer-owned HSMs is performed only by direction of the customer, and only under dial control. Such inspections are reviewed to ensures all customer-identified inspections occur.	Customers are responsible for requesting inspection of customer-owned HSMs, including all required tests as described in this control. Bare Metal Rack HSM customers have the additional option for requesting physical access to customer-owned HSMs hosted in dedicated racks to perform this quarterly inspection.
4C-1.2: Mechanisms must be implemented to detect and respond to suspicious activity, including but not limited to: • Physical breach • Tampered, missing, or substituted devices • Unauthorized logical alterations (e.g.,	Google is responsible for providing mechanisms to detect and respond to suspicious physical activity, including physical breach; tampered, missing, or substituted devices, and physical disconnect/reconnect of devices in the facility where customer-owned HSMs are deployed.	Customers are responsible for providing mechanisms to detect and respond to suspicious logical activity, such as unauthorized logical alterations, unauthorized use of sensitive functions, logical disconnect/reconnect of devices, failure of any device security control, encryption/decryption failures, and unauthorized use of the HSM API.

PCI P2PE REQUIREMENT	Google Responsibility	Customer ResponsIbility
configurations, access controls) • Unauthorized use of sensitive functions (e.g., key-management functions) • Disconnect/reconnect of devices • Failure of any device security control • Encryption/decryption failures • Unauthorized use of the HSM API	Coalfire reviewed incident response procedures and observed a sample alarm triggered and logged during a simulation of an intrusion. During the onsite and virtual walkthroughs, the Google authorized employee forced open the entrance to the area where HSMs were stored to demonstrate the control is in place for applicable scenarios. Coalfire observed the event logged and reviewed by the operations team.	Customers are responsible for physical and logical security of systems not managed within the GCP environment.
29-1: Secure cryptographic devices—such as HSMs and POI devices—must be placed into service only if there is assurance that the equipment has not been subjected to unauthorized modifications, substitution, or tampering and has not otherwise been subject to misuse prior to deployment.	Coalfire observed through interviews with staff that HSMs are inspected prior to deployment to verify that the equipment is intact and has not been modified or tampered with.	Customers are responsible for physical and logical security of systems not managed within the GCP environment.
29-4: Dual-control mechanisms must exist to prevent substitution or tampering of HSMs—both deployed and spare or backup devices—throughout their lifecycle. Procedural controls, which may be a combination of physical barriers and logical controls, may exist to support the prevention and detection of substituted HSMs, but cannot supplant the implementation of dual-control mechanisms.	Coalfire observed during onsite and virtual walkthroughs that Bare Metal Rack HSM and Bare Metal HSM racks and/or cage doors are controlled by badge access and only authorized individuals can access the racks. Google leverages access controls and strict work authorization procedures to restrict personnel from accessing these areas except under dual control. Only authorized Google personnel are allowed to perform physical installation, rebooting, and decommissioning of devices on the customer's behalf, and dual control is maintained throughout this process. Review of audit logs of badge access confirms all such access is under dual control. Google only needs to physically access the device to conduct the following functions, when requested by customer: • Install the device on the rack and connect network cables and the power supply. • Decommission the device to remove it and either send it	Customers are responsible for providing Google with lists of HSMs sent to the facility location hosting the Google customer-owned HSM solutions, including model names and serial numbers. In addition, the customer must send such documentation via separate channel from the HSM shipment to ensure this control is met. Customers are responsible for physical and logical security of systems not managed within the GCP environment.

PCI P2PE REQUIREMENT	Google Responsibility	Customer ResponsIbility
	back to the customer or destroy it. • Rebooting the device at the customer's request, when necessary.	
29-4.1: HSM serial numbers must be compared to the serial numbers documented by the sender (sent using a different communication channel from the device) to ensure device substitution has not occurred. A record of device serial-number verification must be maintained. ***Note:*** *Documents used for this process must be received via a different communication channel—i.e., the control document used must not have arrived with the equipment. An example of how serial numbers may be documented by the sender includes but is not limited to manufacturer's invoice or similar document.*	Google is responsible to perform HSM serial number comparison during device receipt and installation, based on the information the customer provides. Coalfire verified through review of physical security policy documentation and interviews with staff that devices are tracked by model and serial number and matched with the list sent by the customer.	Customers are responsible for providing Google with lists of HSMs sent to the facility location hosting the Google customer-owned HSM solutions, including model names and serial numbers. In addition, the customer must send such documentation via separate channel from the HSM shipment to ensure this control is met.
29-4.4: Inspect and test all HSMs—either new or retrieved from secure storage—prior to installation to verify devices have not been tampered with or compromised.	Coalfire observed through structured walkthrough with product and facility staff, that HSM seals are inspected prior to installation to verify that devices have not been tampered with.	Customers are responsible to ensure HSMs are packed in tamper-evident packaging before shipping to GCP facility location. Customers can request initial installation physical inspection results to be provided to their assessors if the Google customer-owned HSM solutions are utilized for use within the P2PE environment. Customers are responsible for monitoring suspicious activity on the HSM via logical access to the device.
29-5: Maintain HSMs in tamper-evident packaging or in secure storage until ready for installation.	Google is responsible for ensuring that staff at its colocation provider location that receive HSMs keep them in sealed, tamper-evident packaging until they receive instructions from the customer to install the devices. Coalfire reviewed physical security policies and procedures and interviewed staff to verify that HSMs are kept in the required packaging until the	Customers are responsible for shipping HSMs within tamper-evident packaging for HSMs shipped to the colocation provider location. Customers are responsible for physical and logical security of systems not managed within the GCP environment.

PCI P2PE REQUIREMENT	Google Responsibility	Customer ResponsIbility
	staff receives instructions for installation.	
31-1: Procedures must be in place to ensure that any SCDs to be removed from service—e.g., retired or returned for repair—are not intercepted or used in an unauthorized manner, including rendering all secret and private keys, key material, and account data stored within the device irrecoverable.	Google is responsible for ensuring documented physical security procedures are in place for decommissioning all HSMs removed from the colocation provider location, including destruction of the device when necessary. Coalfire verified through interviews with staff that procedures are in place to securely decommission HSMs needing to be removed from the colocation provider location.	Customers are responsible for providing instructions to Google staff on which HSMs to decommission and ship back or destroy. However, customers can rely on Google staff at the colocation provider location to follow Google physical security policies and procedures.
31-1.1: HSMs require dual control (e.g., to invoke the system menu) to implement all critical decommissioning processes.	Google is not responsible for selection of HSMs or configuration of HSM decommissioning options. Google is responsible to perform all critical decommissioning processes under dual control, based on procedural controls.	Customer is fully responsible for logical security and configuration associated with ensuring customer-owned HSMs satisfy this control.

Table 3: Google PCI P2PE Standard Responsibilities Summary for Bare Metal Rack HSM and Bare Metal HSM

PCI PIN Responsibilities

Entities eligible for assessing against PCI PIN standard can utilize the Google Bare Metal Rack HSM and Bare Metal HSM solutions to help meet HSM needs and provide physical security for the HSMs hosted within Google cloud environment. The remote access management of the customer-owned HSMs that are hosted in the Google cloud environment are the responsibility of the customer and all physical security controls apply for the devices used to perform remote management of HSMs.

The below is a breakdown of the specific PCI PIN requirements in scope for physical security and the respective responsibilities for both Google and its customer using the Google customer-owned HSM solutions. The remaining requirements are not in scope for this review and, as a result , were not included in this list:

PCI PIN REQUIREMENT	Google Responsibility	Customer ResponsIbility
29-1: Secure cryptographic devices—such as HSMs and POI devices (e.g., PEDs and ATMs)—must be placed into service only if there is assurance that the equipment has not been subject to	Coalfire observed through interviews with staff that HSMs are inspected prior to deployment to verify that the equipment is intact and has not been modified or tampered with.	Customers are responsible for physical and logical security of systems not managed within the GCP environment.

PCI PIN REQUIREMENT	Google Responsibility	Customer ResponsIbility
unauthorized modification, substitution, or tampering and has or is not otherwise been subject to misuse prior to deployment. ***Note:*** *This applies to SCDs used for key injection or code signing, including display prompts*		
29-4: Dual-control mechanisms must exist to prevent substitution or tampering of HSMs—both deployed and spare or backup devices—throughout their lifecycle. Procedural controls, which may be a combination of physical barriers and logical controls, may exist to support the prevention and detection of substituted HSMs, but cannot supplant the implementation of dual-control mechanisms.	Coalfire observed during onsite and virtual walkthroughs that Bare Metal Rack HSM and Bare Metal HSM racks and/or cage doors are controlled by badge access and only authorized individuals can access the racks. Google leverages access controls and strict work authorization procedures to restrict personnel from accessing these areas except under dual control. Only authorized Google personnel are allowed to perform physical installation, rebooting, and decommissioning of devices on the customer's behalf, and dual control is maintained throughout this process. Review of audit logs of badge access confirms all such access is under dual control. Google only needs to physically access the device to conduct the following functions, when requested by customer: • Install the device on the rack and connect network cables and the power supply. • Decommission the device to remove it and either send it back to the customer or destroy it. • Rebooting the device at the customer's request, when necessary.	Customers are responsible for providing Google with lists of HSMs sent to the facility location hosting the Google customer-owned HSM solutions, including model names and serial numbers. In addition, the customer must send such documentation via separate channel from the HSM shipment to ensure this control is met. Customers are responsible for physical and logical security of systems not managed within the GCP environment.
29-4.1: HSM serial numbers must be compared to the serial numbers documented by the sender (sent using a different	Google is responsible to perform HSM serial number comparison during device receipt and installation, based on the information the customer provides.	Customers are responsible for providing Google with lists of HSMs sent to the facility location hosting the Google customer-owned HSM solutions,

PCI PIN REQUIREMENT	Google Responsibility	Customer ResponsIbility
communication channel from the device) to ensure device substitution has not occurred. A record of device serial-number verification must be maintained. ***Note:*** *Documents used for this process must be received via a different communication channel—i.e., the control document used must not have arrived with the equipment. An example of how serial numbers may be documented by the sender includes but is not limited to manufacturer's invoice or similar document.*	Coalfire verified through review of physical security policy documentation and interviews with staff that devices are tracked by model and serial number and matched with the list sent by the customer.	including model names and serial numbers. In addition, the customer must send such documentation via separate channel from the HSM shipment to ensure this control is met.
29-4.4: Inspect and test all HSMs—either new or retrieved from secure storage—prior to installation to verify devices have not been tampered with or compromised.	Coalfire observed through structured walkthrough with product and facility staff, that HSM seals are inspected prior to installation to verify that devices have not been tampered with.	Customers are responsible to ensure HSMs are packed in tamper-evident packaging before shipping to GCP facility location. Customers can request initial installation physical inspection results to be provided to their assessors if the Google customer-owned HSM solutions are utilized for use within the P2PE environment. Customers are responsible for monitoring suspicious activity on the HSM via logical access to the device.
29-5: Maintain HSMs in tamper-evident packaging or in secure storage until ready for installation.	Google is responsible for ensuring that staff at its colocation provider location that receive HSMs keep them in sealed, tamper-evident packaging until they receive instructions from the customer to install the devices. Coalfire reviewed physical security policies and procedures and interviewed staff to verify that HSMs are kept in the required packaging until the staff receives instructions for installation.	Customers are responsible for shipping HSMs within tamper-evident packaging for HSMs shipped to the colocation provider location. Customers are responsible for physical and logical security of systems not managed within the GCP environment.
31-1: Procedures must be in place to ensure that any SCDs to be removed from service—e.g., retired or returned for repair—are not intercepted or used in an unauthorized manner, including rendering all secret and private	Google is responsible for ensuring documented physical security procedures are in place for decommissioning all HSMs removed from the colocation provider location, including destruction of the device when necessary.	Customers are responsible for providing instructions to Google staff on which HSMs to decommission and ship back or destroy. However, customers can rely on Google staff at the colocation provider location to follow Google physical security policies and procedures.

PCI PIN REQUIREMENT	Google Responsibility	Customer ResponsIbility
keys, key material, and account data stored within the device irrecoverable.	Coalfire verified through interviews with staff that procedures are in place to securely decommission HSMs needing to be removed from the colocation provider location.	
31-1.1: HSMs require dual control (e.g., to invoke the system menu) to implement all critical decommissioning processes.	Google is not responsible for selection of HSMs or configuration of HSM decommissioning options. Google is responsible to perform all critical decommissioning processes under dual control, based on procedural controls. Coalfire confirmed through interview with product and facility staff that all decommissioning processes are performed under dual control.	Customer is fully responsible for logical security and configuration associated with ensuring customer-owned HSMs satisfy this control.
31-1.5: Devices are tracked during the return process	When Google security policies allow for shipping of HSMs to customer-approved locations (e.g., when it may be confirmed that devices have been fully returned to factory state), Google is responsible to ship devices using trackable process. Coalfire confirmed through interview with product and facility staff that devices are shipped using trackable couriers only.	Customer is fully responsible for logical security and configuration associated with ensuring customer-owned HSMs satisfy this control.
31-1.6: Records of the tests and inspections are maintained for at least one year.	Google is responsible to maintain records of all Google activities for at least one year. Coalfire reviewed audit logs and confirmed that all activities are maintained for at least two years.	Customer is responsible to maintain records of all customer-initiated activities in compliance with this control. Bare Metal Rack HSM customers who perform inspections on customer-owned equipment must be aware that Google may not have knowledge or maintain records of such activities, and it is the customer's responsibility to maintain records detailing these inspections.

Table 4: Google PCI PIN Standard Responsibilities Summary for Bare Metal Rack HSM and Bare Metal HSM

Conclusion

Coalfire conducted a thorough analysis of the impact on compliance for four Payment Card Industry Security Standards Council (PCI SSC) standards (PCI DSS, PCI 3DS, PCI P2PE and PCI PIN) and found that the implementations of the Google Bare Metal Rack HSM and Bare Metal HSM solutions have sufficient controls to meet the physical security requirements when deployed in a compliant manner in a Google-managed facility.

In addition, since Google has no logical access to the HSMs and its physical access is limited to receiving devices, installing them physically within its production environment, providing network and power cabling, and routing network traffic to the devices, the compliance scope is further reduced.

References

- Google Compliance Offerings | PCI DSS https://cloud.google.com/security/compliance/pci-dss
- PCI Data Security Standard (PCI DSS) Requirements and Testing Procedures v4.0:
  https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf
- PCI 3-D Secure (3DS) Core Security Requirements and Assessment Procedures v1.0:
  https://docs-prv.pcisecuritystandards.org/3DS/Standard/PCI-3DS-Core-Security-Standard-v1.pdf
- PCI 3-D Secure (3DS) Core: Technical FAQs for use with Version 1.x:
  https://docs-prv.pcisecuritystandards.org/3DS/Frequently%20Asked%20Questions%20(FAQ)/PCI_3DS_Core_v1.x_Technical_FAQs_Sep2023.pdf
- PCI 3DS Data Matrix v1.1:
  https://docs-prv.pcisecuritystandards.org/3DS/Standard/PCI-3DS-Data-Matrix-v1_1.pdf
- PCI Point-to-Point Encryption (P2PE) Security Requirements and Testing Procedures v3.1:
  https://docs-prv.pcisecuritystandards.org/P2PE/Standard/PCI-P2PE-v3_1-Standard.pdf
- PCI PIN Security Requirements and Testing Procedures v3.1:
  https://docs-prv.pcisecuritystandards.org/PIN/Standard/PCI_PIN_Security_Requirements_Testing_v3_1.pdf

About the authors

Sam Pfanstiel | Principal

As Principal in the Industry Solutions team at Coalfire, Sam is responsible for providing advisory and assessment services for P2PE, PIN, and 3DS solutions and components; performing SSF application security assessments; and identifying the security and compliance impacts of innovative payment technologies for merchants and providers. Sam has been a key member of the Coalfire payments team for five years, bringing a quarter-century of experience in a broad spectrum of disciplines; including payments, security, compliance, fraud, application development, mobile technology, infrastructure, and cryptography. Prior to Coalfire, Sam has held roles of Director of IT, Director of Security Consulting, CIO, and CEO.

Bhavna Sondhi | Director

Bhavna Sondhi is the practice subject matter expert for the Enterprise-Technical Solutions group at Coalfire. Bhavna performs advisory work and leads assessments for various compliance frameworks including PCI DSS, PCI 3DS, PCI SSF, HIPAA, GDPR, CCPA, FINMA, NYDFS and authors technical white papers. Bhavna joined Coalfire in 2014 and brings over 14 years of software engineering and information security experience to the team. Her software engineering experience plays a vital part in ensuring that teams recognize the importance of secure code development and information security within their operational practices.

Published May 2024.

ABOUT COALFIRE

Coalfire is the trusted cybersecurity advisor that helps private and public sector organizations avert threats, close gaps, and effectively manage risk. By providing independent and tailored advice, assessments, technical testing, and cyber engineering services, we help clients develop scalable programs that improve their security posture, achieve their business objectives, and fuel their continued success. Coalfire has been a cybersecurity thought leader for over 20 years and has offices throughout the United States and Europe. For more information, visit Coalfire.com.