WHITE PAPER

GOOGLE CLOUD PLATFORM

FOR PCI 3DS

BHAVNA SONDHI | 3DS, QSA (P2PE), PA-QSA(P2PE),
CISA, ISO/IEC 27001 LEAD IMPLEMENTER,
SECURE SOFTWARE AND SECURE SLC ASSESSOR

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 (QSA) and PCI Three-Domain Secure (PCI 3DS) assessor company, to conduct an assessment of their Google Cloud (formerly referred as Google Cloud Platform (GCP)) against the PCI 3DS Core Security Standard

Coalfire conducted assessment activities including document reviews, staff interviews, and data center assessments to validate the Google Cloud environment against PCI 3DS Core Security Standard 1.0 from 9 Feb 2021 – 11 June 2021. An Attestation of Compliance (AOC) document for the assessed PCI 3DS environment was provided to the Google compliance team on 21 July 2021. Coalfire determined that Google Cloud does not have a PCI 3-D Secure Environment (3DE) of its own and only supports the 3DE of customers.

Google Cloud provides infrastructure as a service (IaaS), platform as a service (PaaS), and serverless computing environments for customers to host their own 3DE; however, Google Cloud does not develop or provide 3DS component-hosted services to customers or end users.

The goal of this whitepaper is to provide guidance to customers for hosting their PCI 3DE on Google Cloud and to discuss the applicability of the PCI 3DS Core Security Standard for Google Cloud, including the responsibilities that customers share when hosting their PCI 3DE on Google Cloud.

This paper provides an overview of the 3DS domains, examines the relationship between the PCI Data Security Standard (DSS) and 3DS Core Security Standard, and defines the responsibilities shared by Google Cloud and its customers to meet the 3DS Core Security Standard requirements. Google provides a PCI 3DS responsibility matrix and PCI 3DS AOC for their Google Cloud environment through the Google compliance team. Customers can request documentation that outlines the responsibilities shared by Google Cloud and the 3DS entity and that confirms Google Cloud’s compliance with applicable PCI 3DS requirements.

WHAT IS 3DS?

3DS is a specification, based on an Extensible Markup Language (XML) messaging protocol, that enables cardholders to authenticate themselves with their card issuer for card-not-present online transactions. The specification aims at securing authentication and identity verification in mobile- and browser-based applications. 3DS is defined within the Europay, Mastercard, and Visa (EMV) 3DS Protocol and Core Functions Specification document, which is managed and maintained by EMVCo.

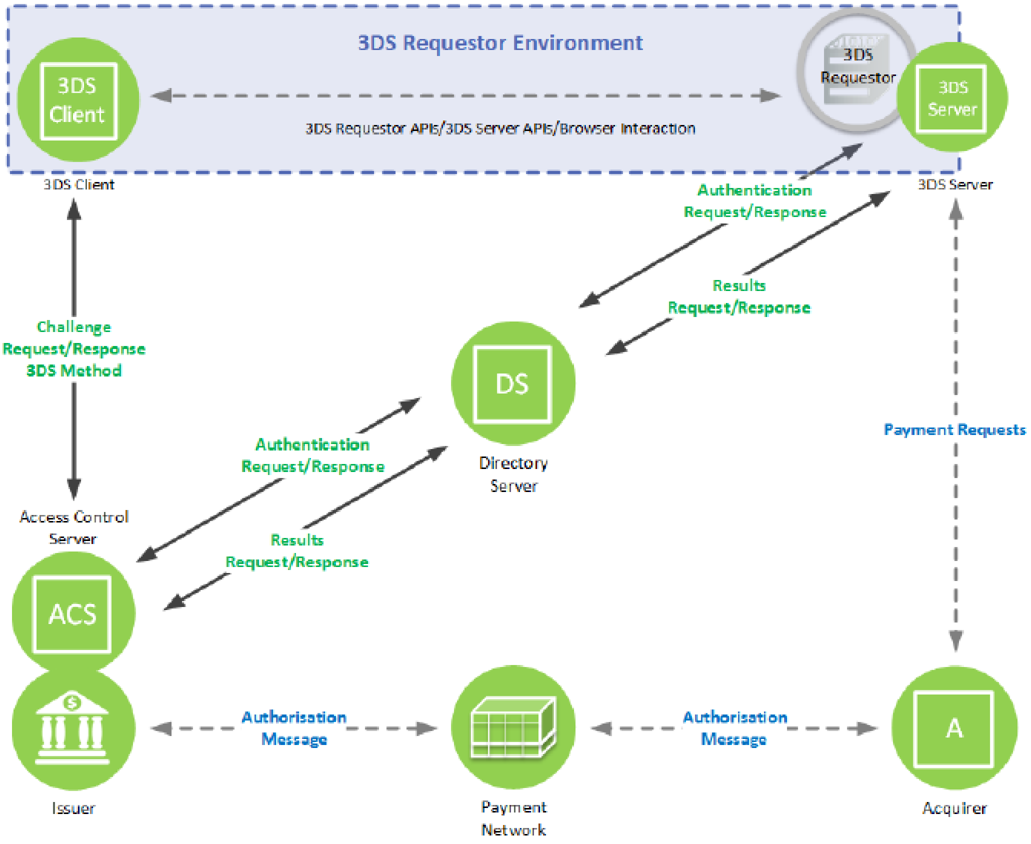
The following three domains are included within 3DS[1]:

- **Acquirer Domain** – 3DS transactions are initiated from the acquirer domain. The components under this domain are the 3DS requester environment, the 3DS integrator, and the acquirer.
- **Interoperability Domain** – The interoperability domain facilitates the transfer of transaction information between the acquirer domain and the issuer domain. The components under this domain are the Directory Server (DS), the Directory Server Certificate Authority (DS-CA), and the authorization system.

[1] https://www.emvco.com/terms-of-use/?u=/wp-content/uploads/documents/EMVCo_3DS_Spec_v220_122018.pdf

- **Issuer Domain** – 3DS transactions are authenticated in the issuer domain. The components under this domain are the cardholder, the consumer device, the issuer, and the Access Control Server (ACS).

Figure 1 below depicts the interaction between the three domains and their components:



Note: Dashed arrows and 3DS Requestor are not part of 3DS specification and are shown for clarity only

Figure 1: 3-D Secure Domains and Components[2]

3DS Transaction Overview

- **Step 1** – Consumer's payment information is transmitted to the 3DS Client from the consumer device. The 3DS Client interfaces with the 3DS Server (3DSS), retrieving the necessary data elements and forming the 3DS messages. The 3DSS also ensures the protection of the message content.
- **Step 2** – 3DS messages are processed by integrating with the DS. The DS authenticates the 3DSS and routes the messages containing transaction data between the 3DSS and ACS. The acquirer sends the requests to the issuer via the authorization system. This system also ensures the responses from the issuer are returned to the acquirer.
- **Step 3** – As part of the final step in authorization, a 3DS transaction occurs within the ACS. The primary functions of the ACS include:

  a. Verifying whether 3DS authentication is available for a particular card number.

[2] https://www.emvco.com/terms-of-use/?u=/wp-content/uploads/documents/EMVCo_3DS_Spec_v220_122018.pdf

b. Authenticating the specific cardholder for the transaction once a card is validated as eligible for the transaction.

c. Sending a response back to the requester environment after the cardholder is validated and approved.

PCI 3DS Core Security Standard and Applicability

The PCI 3DS Core Security Standard applies to environments where 3DS ACS, DS, or 3DSS functions are performed. A 3DE contains the system components involved in performing or facilitating 3DS transactions. Other components that make up the 3DE include network devices, servers, applications, and computing devices.

PCI 3DS Core Security Standard 1.0 page 11, Use of Third-Party Service Providers/Outsourcing Option (a) specifies the following:

"While the ultimate responsibility for the security of the 3DE and 3DS Data lies with the 3DS entity, service providers may be required to demonstrate compliance with the applicable PCI 3DS requirements based on the provided service. The service provider may do so by undergoing a PCI 3DS assessment and providing evidence to its 3DS entity customers to demonstrate its compliance to applicable PCI 3DS requirements."

Google Cloud acts as a service provider to 3DS entities and offers Hardware Security Module (HSM) hosting and data center environments for the hosting of infrastructure and services. Therefore, Google Cloud was eligible to be validated for the applicable PCI 3DS Core Security Standard requirements. Google Cloud products can be utilized by 3DS customers to host their 3DE as well as to meet certain applicable controls related to physical security within data center environments. There are various shared controls, and 3DS entities are required to ensure that they configure and utilize the Google Cloud products in a manner that meets all applicable PCI 3DS requirements.

The PCI 3DS Core Security Standard defines the following functions performed or provided by EMV 3DS entities[3]:

- **3DS ACS** – Contains the authentication rules and is managed within the issuer domain.
- **3DSS** – Provides the functional interface between the 3DS requester environment and the DS.
- **3DS DS** – Maintains a list of valid card ranges for which authentication may be available and coordinates communication between the 3DSS and the ACS systems to determine whether authentication mechanisms are available for a particular card number and device type.

For more information on the functions performed by the ACS, DS, and 3DSS, please refer to the EMVCo 3DS Protocol and Core Functions Specification and the PCI 3DS Core Security Standard.

PCI DSS AND PCI 3DS CORE SECURITY STANDARD

The PCI DSS and PCI 3DS Core Security Standard are independent standards. The PCI DSS environment is validated by PCI QSA, and the PCI 3DS environment is validated by a PCI 3DS assessor with qualifications criteria unique to that program. A 3DE can either be a part of a PCI cardholder data environment (CDE) or a completely separate environment. The payment brand will determine if an entity is required to comply with PCI 3DS Core Security Standard requirements, PCI DSS, or both.

Google Cloud offers products, outlined in the Google Cloud 3DS Products table, that can be used to support customers' solutions for 3DS functions. Google Cloud does not perform the functions of 3DSS, DS, or ACS

[3]

directly, but instead supports elements of a PCI 3DS Combined Environment, as shown in Figure 2 below. Google Cloud can support both a PCI 3DS Standalone Environment and a PCI 3DS Combined Environment for when responsibilities are shared between Google Cloud and the customer. The PCI 3DS Standalone Environment applies to customers who are not eligible for validation under PCI DSS and only eligible to be validated under PCI 3DS Core Security Standard that covers PCI 3DS Part 1 and PCI 3DS Part 2 .

The PCI 3DS Core Security Standard requirements are organized into two parts:

- **Part 1: Baseline Security Requirements** – A baseline of technical and operational security requirements designed to protect the 3DE.
- **Part 2: 3DS Security Requirements** – The security requirements designed to protect 3DS data and processes.

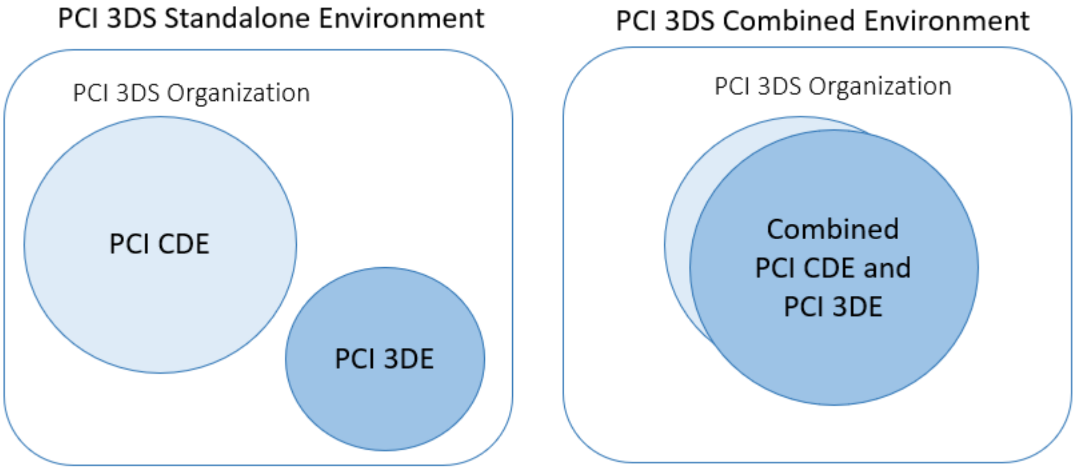

PCI 3DS Standalone Environment
PCI 3DS Organization
PCI CDE
PCI 3DE
PCI 3DS Combined Environment
PCI 3DS Organization
Combined PCI CDE and PCI 3DE

Figure 2: 3DE Scenarios

GOOGLE CLOUD 3DS PRODUCTS

The following products are provided by Google Cloud to customers to support their PCI 3DS environments:

GOOGLE CLOUD PRODUCTS	DESCRIPTION	DOCUMENTATION
Cloud Key Management Service (KMS)	Cloud Key Management Service is a cloud-hosted key management service that lets you manage cryptographic keys for your cloud services the same way you do on premises. You can generate, use, rotate, and destroy AES256, RSA 2048, RSA 3072, RSA 4096, EC P256, and EC P384 cryptographic keys.	https://cloud.google.com/security/key-management-deep-dive https://cloud.google.com/kms/docs

GOOGLE CLOUD PRODUCTS	DESCRIPTION	DOCUMENTATION
Cloud HSM	Cloud HSM (Hardware Security Module) is a cloud-hosted key management service that lets you protect encryption keys and perform cryptographic operations within a managed HSM service. You can generate, use, rotate, and destroy various symmetric and asymmetric keys. *Note: Please see Table 2 for use cases for Cloud HSM. Please discuss the possible implementation options with Google.*	https://cloud.google.com/kms/docs/hsm
Google Kubernetes Engine (GKE)	Google Kubernetes Engine, powered by the open source container scheduler Kubernetes, enables you to run containers on Google Cloud Platform. Kubernetes Engine takes care of provisioning and maintaining the underlying virtual machine cluster, scaling your application, and operational logistics such as logging, monitoring, and cluster health management.	https://cloud.google.com/kubernetes-engine/docs/how-to
Google Compute Engine (GCE)	Compute Engine offers scalable and flexible virtual machine computing capabilities in the cloud, with options to utilize certain CPUs, GPUs, or Cloud TPUs. You can use Compute Engine to solve large-scale processing and analytic problems on Google's computing, storage, and networking infrastructure.	https://cloud.google.com/compute/docs/how-to
BigQuery	BigQuery is a fully managed data analysis service that enables businesses to analyze Big Data. It features highly scalable data storage that accommodates up to hundreds of terabytes, the ability to perform ad hoc queries on multi-terabyte datasets, and the ability to share data insights via the web.	https://cloud.google.com/bigquery/docs/how-to
Cloud SQL	Cloud SQL is a web service that allows you to create, configure, and use relational databases that live in Google's cloud. It is a fully managed service that maintains, manages, and administers your databases, allowing you to focus on your applications and services.	https://cloud.google.com/sql/docs/mysql/how-to
Cloud Spanner	Cloud Spanner is a fully managed, mission-critical relational database service. It is designed to provide a scalable online transaction processing (OLTP) database with high availability and strong consistency at global scale.	https://cloud.google.com/spanner/docs/how-to

GOOGLE CLOUD PRODUCTS	DESCRIPTION	DOCUMENTATION
Dataflow	Dataflow is a fully managed service for strongly consistent, parallel data-processing pipelines. It provides an SDK for Java with composable primitives for building data-processing pipelines for batch or continuous processing. This service manages the life cycle of Compute Engine resources of the processing pipeline(s). It also provides a monitoring user interface for understanding pipeline health.	https://cloud.google.com/dataflow/docs/how-to
Dataproc	Dataproc is a fast, easy to use, managed Spark and Hadoop service for distributed data processing. It provides management, integration, and development tools for unlocking the power of rich open source data processing tools. With Dataproc, you can create Spark/Hadoop clusters sized for your workloads precisely when you need them.	https://cloud.google.com/dataproc/docs/how-to
Google Cloud Storage	Cloud Storage is a RESTful service for storing and accessing your data on Google's infrastructure. The service combines the performance and scalability of Google's cloud with advanced security and sharing capabilities.	https://cloud.google.com/storage/docs/how-to
Hosted Private HSM Solution	Google’s Hosted Private HSM Solution enables select large Cloud customers who are pre-approved by the product team to contract directly with Google for placement of their HSM appliances within specified colocation facilities and to connect to Google Cloud for a monthly fee, with Google providing physical and network security, rack space, power, and network integration. Customer-supplied HSMs store digital keys and perform a variety of cryptographic functions. The placement of Hosted Private HSM capacity is in facilities with active peering fabrics. These hosting centers meet Google’s own data center security standards, as well as PCI 3DS and PCI DSS standards, and provide a low-latency, highly available service. This offering is limited to FIPS 140-2 Level 3 certified HSMs and is not a generalized hosting or colocation service. Google Cloud	https://cloud.google.com/kms/docs/hosted-private-hsm
Pub/Sub	Pub/Sub is designed to provide reliable, many-to-many, asynchronous messaging between applications. Publisher applications can send messages to a "topic" and other applications can subscribe to that topic to receive the messages. By decoupling senders and receivers, Pub/Sub allows developers to communicate between independently written applications.	https://cloud.google.com/pubsub/docs/how-to

GOOGLE CLOUD PRODUCTS	DESCRIPTION	DOCUMENTATION
Cloud Functions	Cloud Functions is a lightweight, event-based, asynchronous compute solution that allows you to create small, single-purpose functions that respond to cloud events without the need to manage a server or a runtime environment.	https://cloud.google.com/functions/docs/how-to

Table 1: Google Cloud Platform Products

3DS SHARED RESPONSIBILITY SUMMARY

Google Cloud 3DS customers are responsible for ensuring that they meet all the 3DS controls for 3DS compliance by configuring and managing the utilized products hosted in Google Cloud. The responsibility for each 3DS requirement can be verified via the PCI DSS Responsibility Matrix section of the Google Cloud Platform: Shared Responsibility Matrix, available from the Google Compliance team upon request. Below are high-level partial responsibilities that Google Cloud shares with its customers:

- Google Cloud offers products identified in the PCI 3DS AOC. All logical security controls required to protect 3DS functions are the responsibility of the customer.
- Google Cloud offers PCI DSS- and PCI-3DS-compliant data center environments where Google Cloud manages the physical security controls.
- Google Cloud offers a Hosted Private HSM solution that allows customers to host and manage their own HSM remotely or within a colocation data center to meet certain PCI 3DS requirements applicable to ACS and DS environments.
- Google Cloud offers a Cloud HSM product for 3DSS environments (for FIPS 140-2 Level 3 certified HSMs only).
- Google Cloud protects infrastructure, including hardware and software; however, customers are required to implement and configure the products as per the 3DS requirements.

The following subsections describe the responsibilities that Google Cloud assumes for the products offered, as well as the customer's responsibilities when utilizing the in-scope Google Cloud products.

PCI 3DS PART 1: BASELINE SECURITY REQUIREMENTS

As Google Cloud is hosted in PCI DSS CDE, Google Cloud leverages PCI DSS compliance to help meet PCI 3DS Core Security Standard Part 1 requirements. Google Cloud customers are, however, responsible for complying with all 3DS Part 1 requirements. Customers hosting within the Google Cloud environment share certain responsibilities with Google, and, to maintain their 3DS compliance, they should be aware of the following information:

- **Google Cloud PCI DSS and PCI 3DS AOC** – The AOC documents for Google Cloud are made available by the Google Compliance team to confirm Google Cloud's compliance for the products offered.
- **Google Cloud PCI DSS and PCI 3DS Responsibility Matrix** – The shared responsibility matrix identifies the responsibilities shared between Google Cloud and its customers.
- **Contracts and Agreements** – Written contracts and agreements with Google Cloud are required to ensure that security responsibilities are understood and acknowledged by each entity. In

accordance with PCI DSS v3.2.1 requirement 12.8.4, customers should maintain a program to monitor service providers' compliance status at least annually.

- **Implementation of Products** – Google Cloud customers should identify the in-scope products and ensure that they are implemented and configured in accordance with Google Cloud guidelines, as well as in compliance with PCI requirements.

PCI 3DS PART 2: SECURITY REQUIREMENTS TO PROTECT 3DS DATA AND PROCESSES

Google Cloud's 3DS environment meet the applicable requirements identified within PCI 3DS Part 2, as demonstrated in PCI 3DS AOC, but there are responsibilities that are partially shared with the customer for the products it offers. It is important for customers to retrieve the following documents in order to understand the products offered by Google Cloud for PCI 3DS and to become aware of customer responsibilities for meeting controls:

- **Google Cloud PCI 3DS Responsibility Matrix** – This document outlines the in-scope Google Cloud products that can be used to meet Part 2 of the 3DS Core Security Standard requirements. There are various responsibilities shared between Google Cloud and its customers. The products utilized are required to be configured in accordance with guidance provided by Google in order to meet 3DE requirements. The responsibility matrix documents are available from the Google Compliance team.
- **Google Cloud PCI 3DS AOC** – The current PCI 3DS attestation document for validated compliance frameworks is available from the Google Compliance team.

The high-level 3DS Part 2 Requirements, PCI DSS corresponding requirements, and the responsibilities of Google Cloud and Google Cloud customers are outlined below. Please refer to Google Cloud Platform: Shared Responsibility Matrix for additional information.

3DS PART 2 REQUIREMENTS			RESPONSIBILITY SUMMARY
P2-1	Validate scope	1.1 Scoping	**Google Cloud:** Google Cloud provides a platform for 3DS implementation by the customer and does not directly store, process, or transmit 3DS data. Google Cloud has identified 3DS in-scope products that are hosted for supporting customer's 3DE. The Google Cloud environment includes infrastructure, development, operations, management, support, and the in-scope products. **Customers:** Google Cloud customers are responsible for identifying their scope for PCI 3DE, including connectivity from their corporate environments.
P2-2	Security governance	2.1 Security governance 2.2 Manage risk 2.3 Business as usual (BAU) 2.4 Manage third-party relationships	**Google Cloud:** Google Cloud meets the applicable controls for their environment as identified within the PCI 3DS AOC. **Customers:** Google Cloud customers must have their own security governance, risk management, and review and monitoring processes, as well as third-party process management, in place.
P2-3	Protect 3DS systems and applications	3.1 Protect boundaries 3.2 Protect baseline configurations 3.3 Protect applications and application interfaces	**Google Cloud:** Google Cloud meets the applicable controls for their environment as identified within the PCI 3DS AOC. However, some controls are specific to managing traffic between 3DS components, and Google Cloud does not directly handle those services.

3DS PART 2 REQUIREMENTS			RESPONSIBILITY SUMMARY
		3.4 Secure web configurations 3.5 Maintain availability of 3DS operations	The below documentation provides the security design overview of the Google Infrastructure and Google's approach to security and compliance for Google Cloud: Google Cloud Security Design Whitepaper Google Cloud Security Whitepaper **Customers:** Google Cloud customers are responsible for implementing the in-scope products per Google Cloud guidelines to meet the PCI 3DS controls. See the Google Cloud 3DS Products section and the security baseline documentation at the following link for additional details: https://cloud.google.com/docs For maintaining the availability of 3DS operations, refer to following guidance: Regions and Zones Selections CloudSQL High Availability Configuration
P2-4	Secure logical access to 3DS systems	4.1 Secure connections for issuer and merchant customers 4.2 Secure internal network connections 4.3 Secure remote access 4.4 Restrict wireless exposure 4.5 Secure VPNs	**Google Cloud:** Google Cloud meets the applicable controls for their environment as identified within the PCI 3DS AOC. **Customers:** Customers are responsible for configuring both the in-scope products and logical access to the in-scope products for their 3DE. See the Google Cloud 3DS Products section and the security baseline documentation at the following link for additional details: https://cloud.google.com/kubernetes-engine/docs/concepts/cis-benchmarks Additional resources for configurations: • Virtual Private Cloud (VPC) firewall rules • Identity and Access Management
P2-5	Protect 3DS data	5.1 Data lifecycle 5.2 Data transmission 5.3 TLS configuration 5.4 Data storage 5.5 Monitoring 3DS transactions	**Google Cloud:** Google Cloud meets the applicable controls for their environment as identified within the PCI 3DS AOC. **Customers:** Customers are responsible for configuring the in-scope products and for protecting the 3DS data within their 3DE. See the Google Cloud 3DS Products section and the security baseline documentation at the following link for additional details: https://cloud.google.com/architecture/pci-dss-compliance-in-gcp Default encryption is available for the application services offered by Google Cloud. However, configurations are still required to be performed by customers to meet certain compliance framework requirements: • Encryption of data at rest • Encryption of data in transit • Securing Site with HTTPS

3DS PART 2 REQUIREMENTS			RESPONSIBILITY SUMMARY
			Google Cloud offers the following products for data storage: • Compute Engine options, such as persistent disk, local storage, cloud storage buckets. • Cloud Storage, Cloud SQL, Cloud Spanner For 3DSS environments, customers can utilize Cloud HSM or Cloud KMS for key management processes to protect sensitive 3DS data. However, for the ACS and DS 3DE environments the key management processes must be performed on the HSM. Requirements outlined in P2–6.2 Secure Logical Access to HSMs (For ACS and DS only) limit the ability to utilize cloud-based HSM services. Therefore, Cloud HSM is not a recommended solution for ACS and DS environments. Customers must monitor 3DS transactions. Monitoring can be enabled for various products when Google Cloud products are utilized: • Cloud SQL • Dataflow • Dataproc • GCS • Cloud KMS • Pub/Sub • Cloud Functions
P2-6	Cryptography and key management	6.1 Key management 6.2 Secure Logical access to HSMs (For ACS and DS only) 6.3 Secure Physical access to HSMs (For ACS and DS only)	**Google Cloud:** **3DSS Environments:** Google Cloud offers products such as Cloud KMS and Cloud HSM key management for 3DSS. Google Cloud meets the controls applicable for their environment. **ACS and DS Environments**: The key management processes are required to be performed on the HSM. For the Hosted Private HSM solution, customers are fully responsible for managing all types of keys as well as non-console access to the HSM. Google only handles the physical security and segmentation of HSMs. Requirements outlined in P2–6.2 Secure Logical Access to HSMs (For ACS and DS only) limit the ability to utilize cloud-based HSM services. Therefore, Cloud HSM is not a recommended solution for ACS and DS environments. **Customers:** **For 3DSS environments**: Google Cloud customers are responsible for managing all cryptographic key management processes for their own 3DE when utilizing any HSM service. Google Cloud customers are also responsible for securing physical access to the area or room where non-console access to the HSM is initiated. Specifically:

3DS PART 2 REQUIREMENTS			RESPONSIBILITY SUMMARY
			• Cloud KMS – Google Cloud customers are responsible for managing cryptographic keys as identified in the Cloud KMS guidelines. • Cloud HSM – Google Cloud manages the HSM clustering, scaling, and patching and utilizes Cloud KMS as the front end. Google Cloud customers are responsible for handling the cryptographic key management processes specific to the keys created for their environment as identified within Cloud HSM guidelines. **For ACS and DS environments**: Customers can choose to utilize the Hosted Private HSM solution. It is the customer's responsibility to ensure that the HSMs used within the 3DS environment for managing ACS and DS components are PCI PTS-approved or FIPS 140-2 Level 3 (overall) or higher approved. Specifically: • Customers should ensure that they configure the HSMs as per PTS or FIPS security policy, including the provisioning of HSM and securing logical access to HSMs for ACS and the DS 3DS environment as identified within the 3DS requirement. • It is the customer's responsibility to utilize non-console access to the HSM that complies with the current version of International Organization for Standardization (ISO) 13491.
P2-7	Physically secure 3DS systems	7.1 Data center security 7.2 CCTV	**Google Cloud:** Google Cloud maintains the physical security controls for Google data centers and colocations supporting the products within the 3DE and can meet the necessary 3DS requirements for their customers as noted within the PCI 3DS AOC. **Customers:** Google Cloud customers are responsible for managing the physical security of systems not managed within the Google Cloud environment. Google Cloud customers are also responsible for implementing and configuring multi-factor authentication (MFA) controls into telecommunications rooms hosted in their 3DE, as applicable.

Table 2: Google Cloud PCI 3DS Part 2 Requirements Responsibility

IMPLEMENTING WITH GKE

This section provides guidance for the PCI 3DS requirements in Part 2 of the 3DS Core Security Standard and how a Google Cloud environment can assist with achieving compliance when implemented with the GKE product. This guidance is not a turnkey solution; specific configurations must be performed by the customer utilizing Google Cloud for hosting their PCI 3DS environment.

Requirement P2-1: Validate Scope

Guidance: Segmentation is recommended to limit the scope for the PCI DSS and PCI 3DS environment. PCI 3DS can be part of the PCI DSS environment, and it can be segmented from the entity's network to achieve segmentation. The scoping process should involve locations, flows of 3DS data, systems performing 3DS functions, and any systems connected to or that could impact the 3DE. Connected entities and personnel with access to 3DS data should also be identified.

Google Cloud: Segmentation can be achieved on Google Cloud using the following means:

- Logical segmentation using resource hierarchy
- Network segmentation using VPCs and subnets
- Service level segmentation using VPC

For further segmentation using GKE, entities can use namespaces and network policies to partition workloads between clusters.

For more information on how segmentation can be achieved, please see the following:
https://cloud.google.com/architecture/pci-dss-and-gke-guide

Requirement P2-2: Security Governance

Guidance: Security governance programs should identify and define the security objectives, roles and responsibilities, risk management strategy, and third-party relationships procedures for their 3DE. Review and monitoring of procedures for detecting and responding to security control failures should occur periodically.

Google Cloud: Within GKE, configuration of Identity and Access Management (IAM), along with role-based access controls (RBACs), Terraform Config Validator to define constraints for enforcing security and governance policies can assist with achieving governance for use of resources in the 3DE.

Requirement P2-3: Protect 3DS Systems and Applications

Protect boundaries

Guidance: Traffic between 3DS components must be protected and permitted for purposes of 3DS transactions or to support 3DS functions, such as security or management. Various interfaces, including physical, logical, and virtual, must be identified and protected.

Google Cloud: When configuring Google Cloud GKE, the following can assist with boundary protection. 3DS entities should, however, ensure all system types and functions are considered:

- Configure firewall rules on the Compute Engine instances that run GKE nodes, protecting these cluster nodes.
- Configure network policies to restrict flows and protect pods in the cluster.
- Enforce GKE network policy to control communication between cluster pods and services.

- Use encryption, truncation, masking, and hashing in Google Cloud storage buckets, BigQuery instances, Datastore, and Cloud SQL to protect sensitive data.

Protect baseline configurations, applications, and application interfaces

Guidance: Controls such as baseline configuration files, system build data, system images, and build procedures should be implemented to protect data integrity and confidentiality. Processes including change control, strict access controls, and monitoring and programmatic controls can be utilized to ensure the integrity of applications and programs in production.

Google Cloud: Google Cloud provides several guidelines for deploying workloads on GKE cluster that align with PCI DSS. Additional controls for 3DS data and files should be considered while implementing 3DE.

- Follow the principle of least privilege when using Google Cloud resources such as IAM for authorization in GKE.
- Create private GKE cluster where nodes only have internal IP addresses isolating the nodes and Pods from the internet.
- Granular access can be achieved using RBAC.
- Kubernetes control plane components are managed by Google, but the protection of nodes, containers and pods and the securing of those components in GKE is required by the implementing entity.
- GKE deploys workloads on Compute Engine instances within Google Cloud. These instances are attached to the GKE cluster as nodes. The node-level security protection can be achieved using controls identified within the GKE guides.
  Use Shielded GKE nodes feature that provides verifiable node identity and integrity to increase the security of GKE nodes.
- For workloads running in GKE, communication traffic with other services running inside or outside the cluster should be controlled. This can be achieved by:
  - Limiting pod-to-pod communication, see below reference guides:
    https://cloud.google.com/kubernetes-engine/docs/how-to/network-policy,
    https://kubernetes.io/docs/concepts/services-networking/network-policies/#default-deny-all-ingress-and-all-egress-traffic
  - Filtering load balanced traffic, see below reference guides:
    https://cloud.google.com/kubernetes-engine/docs/how-to/internal-load-balancing,
    https://cloud.google.com/load-balancing/docs/network
- Workloads should be secured within GKE by:
  - Limiting pod container process privileges
  - Applying Pod security policies using Gatekeeper to validate requests to create and update Pods on Kubernetes clusters
    Using Workload Identity for Pods that need to access Google Cloud resources

Secure web configurations

Guidance: Application pages and resources should enforce the use of HTTPS and prevent communications over insecure channels. System operations should enable only explicitly required functionality and disable others.

Google Cloud: When utilizing GKE, customers can define ingress rules for routing HTTPS traffic to applications running in the cluster. For applications developed by a customer within Google Cloud, entities can utilize web application firewalls (WAF) such as Cloud Armor, WAFs should be configured to protect the applications from variety of application layer OWASP Top 10 vulnerabilities .

Maintain availability of 3DS operations

Guidance: To maintain the integrity of the 3DS ecosystem, 3DS components should be architected with high availability as a key factor in the software, system, and infrastructure design. The architecture should ensure denial-of-service (DoS) attacks are handled and should not force fallback to a less secure environment. Continuous monitoring should be in place to ensure effectiveness of the availability mechanisms.

Google Cloud: Customers implementing GKE can utilize provided recommendations and best practices to set up GKE clusters for increased availability. High-level design considerations are noted below:

- Choose the right topology for the cluster (e.g., regional or zonal). The regional cluster type is recommended, as it minimizes disruption during control plane maintenance. Setting up the regional cluster with nodes in three different availability zones is recommended.
- Enable the GKE autoscaling capability that best fits customers' needs. Capabilities such as cluster autoscaler, horizontal pod autoscaling, and vertical pod autoscaling can be utilized.
- Configure monitoring settings to observe workload behavior and ensure loading is evenly distributed.
- Utilize Kubernetes Deployments to manage workloads and applications within it.

Requirement P2-4: Secure Logical Access to 3DS Systems

Guidance: The requirement to secure connections is intended for following scenarios:

- The 3DS entity provides issuer and merchant users with access to 3DS services and data through an external party interface, such as an API or web portal.
- Any non-console access to 3DS components (ACS, DS, or 3DSS) utilizes a MFA method that can be applied at the network, system, or application level.
- Any remote access originating from outside the entity's network utilizes MFA.
- All virtual private network (VPN) access to the 3DE should be reviewed against industry-recommended implementations.

Google Cloud: Google provides strong communications and protects against eavesdropping, replay, or man-in-the-middle attacks using the BeyondCorp zero trust model. This provides single sign-on, access control policies, access proxy, and user- and device-based authentication and authorization. MFA can be configured from a Google workspace account to perform two-step verification.

Requirement P2-5: Protect 3DS Data

Data lifecycle and data storage

Guidance: 3DS entities should identify the 3DS-sensitive they handle and apply protection measures based on data sensitivity, legal, and business requirements for the entire lifecycle of 3DS data. The data retention schedules should be defined, and appropriate secure destruction procedures should exist. Please refer to PCI 3DS data matrix to identify the 3DS sensitive data.

Google Cloud: Google offers several storage options for applications running on GKE, such as Cloud SQL, data storage, or Cloud Spanner. When utilizing cloud storage options, refer to best practice guidance from Google Cloud, as well as the PCI 3DS data matrix to ensure that the Cloud storage options utilized only store data permitted by the 3DS Core Security Standard. Google encrypts all customer data at rest by default and utilizes several layers of encryption, including application layer, platform layer, infrastructure layer, and hardware layer. 3DS entities should evaluate the sensitivity and protection of data based on their risk-management policy and configure the applications developed or the Google Cloud products utilized accordingly.

Data transmission

Guidance: 3DS entities should apply controls for all interfaces and locations where 3DS sensitive data is transmitted or received, including data transmitted over open or public networks, internal networks, and transmission within or between 3DS system domains. Use of trusted keys or certificates, secure protocols, and strong cryptography to encrypt 3DS data is essential for secure transmission. Any insecure connections with unsupported encryption strength are not permitted.

Google Cloud: Google offers both encryption by default and user-configurable options for protecting data in transit. Google automatically encrypts traffic between Google Front Ends (GFEs) and backend services residing within the Google Cloud VPC network. However, customers should ensure that the protocols and encryption type that meet the necessary 3DS requirements are configured for use. Google offers the following configurable options to users for protection of data in transit:

- On-premises data center to Google Cloud
- User to GFE
- Service-to-service and VM-to-VM encryption

When configuring TLS communications between ACS, DS, and 3DSS components, TLS v1.2 or higher is required, and the below cipher should be supported as a minimum.

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

The below cipher suites are not allowed or supported in 3DS environments:

- Any cipher suite represented as “Null,” “Anonymous/Anon.”
- Any cipher suite that incorporates any of the algorithms “RC2,” “RC4,” “DES,” “IDEA,” “KRB5,” “ARIA,” or “MD5.”
- Any cipher suite incorporating an export grade algorithm using “EXPORT.”
- 3DES and SHA-1 are to be phased out, so customers are advised against using algorithms that will be unsupported in the near future.

Please refer to the specific EMVCo 3DS Specifications for additional details.

Requirement P2-6: Cryptography and Key Management

Key management

Guidance: The 3DS entities’ policies should cover all cryptographic keys and processes used for protecting confidentiality and integrity of 3DS data and messages during transmission and storage. The data encryption keys and key-encrypting keys require similar protection.

- **ACS and DS entities** – These require the use of an HSM to protect the 3DS cryptographic key types defined within 3DS Data Matrix. PCI SSC recommends the use of HSMs for other 3DS keys not specified within PCI 3DS Data Matrix. All key-management activities, including key-encryption, decryption, and key lifecycle functions (e.g., key generation, loading, and storage), are to be performed on HSM.

  The HSM in use should be either FIPS 140-2 Level 3 or higher certified or PCI PTS HSM approved.
- **3DSS entities** – These do not require the use of an HSM to manage 3DS keys; however, it is strongly recommended.

Google Cloud: Cloud HSM utilizes FIPS 140-2 Level 3 (overall) or higher approved HSMs. Google manages the Cloud HSM and root keys using console access. Any other cryptographic key generation and management is the responsibility of customer.

The Hosted Private HSM Solution offers customers the option of hosting their own HSM (that is least FIPS 140-2 Level 3 certified) at Google colocation data centers. Customers are responsible for the full life cycle key management, as well as any non-console access to HSM using this solution.

Note: Requirements outlined in P2–6.2 Secure Logical Access to HSMs (For ACS and DS only) limit the ability to utilize cloud-based HSM services. Therefore, Cloud HSM is not a recommended solution for ACS and DS environments.

Secure logical access to HSMs

Guidance: Logical access to HSMs requires additional controls to restrict and protect access. Any network (non-console) access to HSMs for purposes of maintenance, configuration, updates, administration, and general management requires additional security measures to be in place. For handling non-console access, both hardware components (i.e., smart cards, network appliances) and software components (i.e., client-side applications) are typically utilized. Non-console access solutions require evaluation by an independent laboratory in accordance with sections of ISO 13491 identified within the PCI 3DS Core Security Standard. It is the customer's responsibility to ensure this has taken place.

Google Cloud:

For 3DSS environments: Google Cloud customers are responsible for managing all cryptographic key management processes for their own 3DE when utilizing any HSM service. Google Cloud customers are also responsible for securing physical access to the area or room where non-console access to the HSM is initiated.

- **Cloud KMS** – Google Cloud customers are responsible for managing cryptographic keys as identified in the Cloud KMS guidelines provided by Google.
- **Cloud HSM** – Google Cloud manages the HSM clustering, scaling, and patching and utilizes Cloud KMS as the front end. Google Cloud customers are responsible for handling the cryptographic key management processes specific to the keys created for their environment when using Cloud HSM.

For ACS and DS environments: Customers can choose to utilize the Hosted Private HSM solution or Cloud HSM.

- Cloud HSM utilizes FIPS 140-2 Level 3 (overall) or higher approved HSM. Google manages the Cloud HSM and root keys using console access.

  PCI 3DS requirements do not allow the loading and exporting of clear-text cryptographic keys, key components, and key shares to or from the HSM over a non-console connection. There may be instances where loading of key components is required, please work with Google to analyze the possible solutions. One example is noted below.

- A 3DS entity can host a FIPS 140-2 Level 3 or PCT PTS HSM approved HSM in a non-Google Cloud environment (own data center or on-premises network) that meets all 3DS requirements for managing the loading and exporting directly on the HSM. They could then use Google Cloud Interconnect for a dedicated connection to an off-cloud network as shown in Figure 3 below.

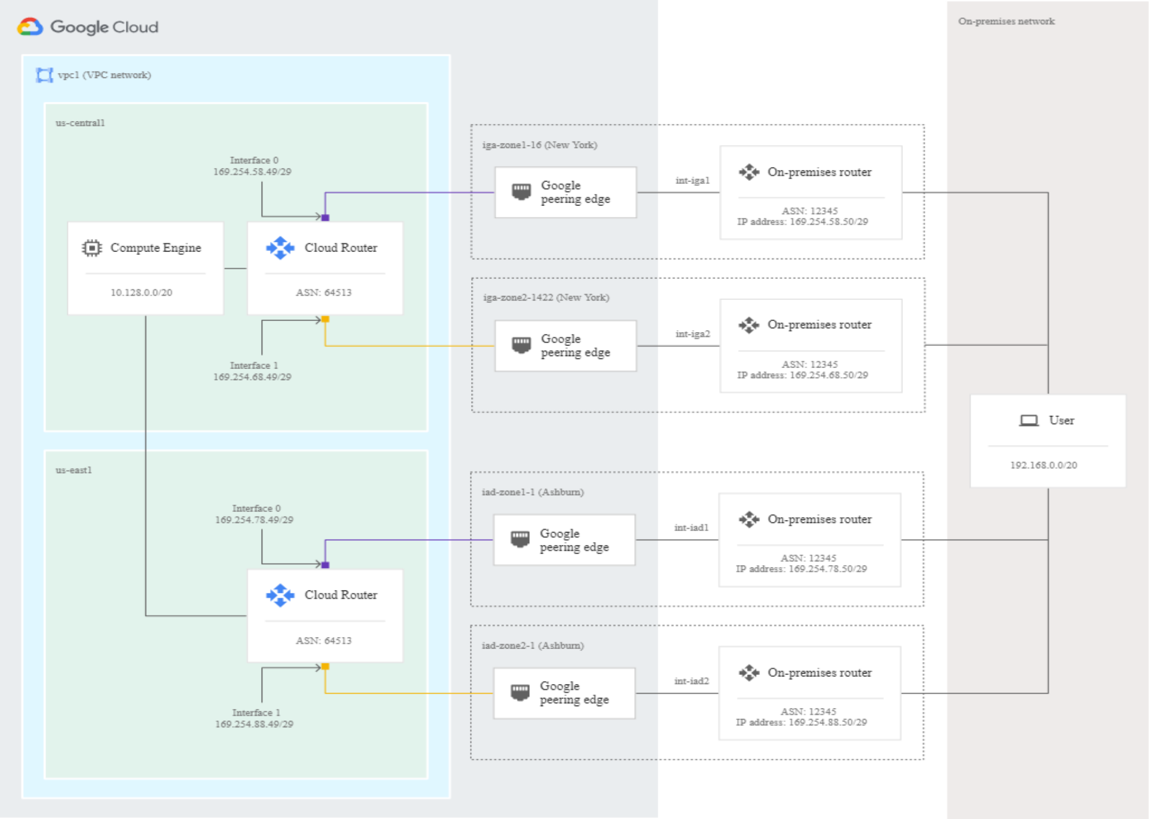


Figure 3: Google Cloud Dedicated Interconnect Architecture

- When using Hosted Private HSM Solution for deployment of HSMs within Google's colocation facility, customers should consider the following.
  - Customers should ensure they configure the HSMs as per PTS or FIPS security policy, including the provisioning of HSM and securing logical access to HSMs for ACS and DS 3DS environments as identified within the 3DS requirement.
  - It is the customer's responsibility to utilize non-console access to the HSM that complies with the current version of ISO 13491 for the allowed purposes.
  - The customer should load any cryptographic keys, key components, and key shares to or from the HSM in a 3DS compliant facility via console connection to HSM. This can be done prior to deployment with Google.

Requirement P2-7: Physically Secure 3DS Systems

Guidance: ACS and DS system components, including their HSMs, are required to be hosted in a data center facility with appropriate physical controls (e.g., card reader, biometric scanner), including positively controlled single-entry portal (e.g., mantrap). The 3DSS system components do not require single-entry access but it is recommended. 3DS environments require physical intrusion detection systems and activation of alarms if the facility is intended to be unoccupied. Use of CCTV cameras that captures footage at all times of the day and night is required for monitoring entry and exit points.

Google Cloud: Customers can use Google Cloud for physical security of 3DE in Google Cloud. For systems not hosted in the cloud, customers should manage their own on-premises network and physical security. Physical security should be maintained for dedicated areas and for rooms that provide non-console access to the HSMs hosted in data center environment.

SAMPLE ARCHITECTURE DIAGRAM FOR DS COMPONENT IN GOOGLE CLOUD

The below diagram demonstrates a sample use case for a company that has implemented a 3DS DS component within their Google Cloud hosted environment.

The EMVCo 3DS Directory service is hosted by an entity within the Google Cloud environment and is integrated with an existing PCI DSS CDE, as shown in the sample 3DS architecture diagram below.

The Directory Server performs the following functions:

- Authenticates the 3DSS and the ACS
- Routes messages between the 3DSS and the ACS
- Validates the 3DSS, the 3DS SDK, and the 3DS Requestor
- Defines specific program rules
- Performs onboarding of 3DSS and ACSs
- Maintains ACS and DS start and end protocol versions and 3DS method URLs

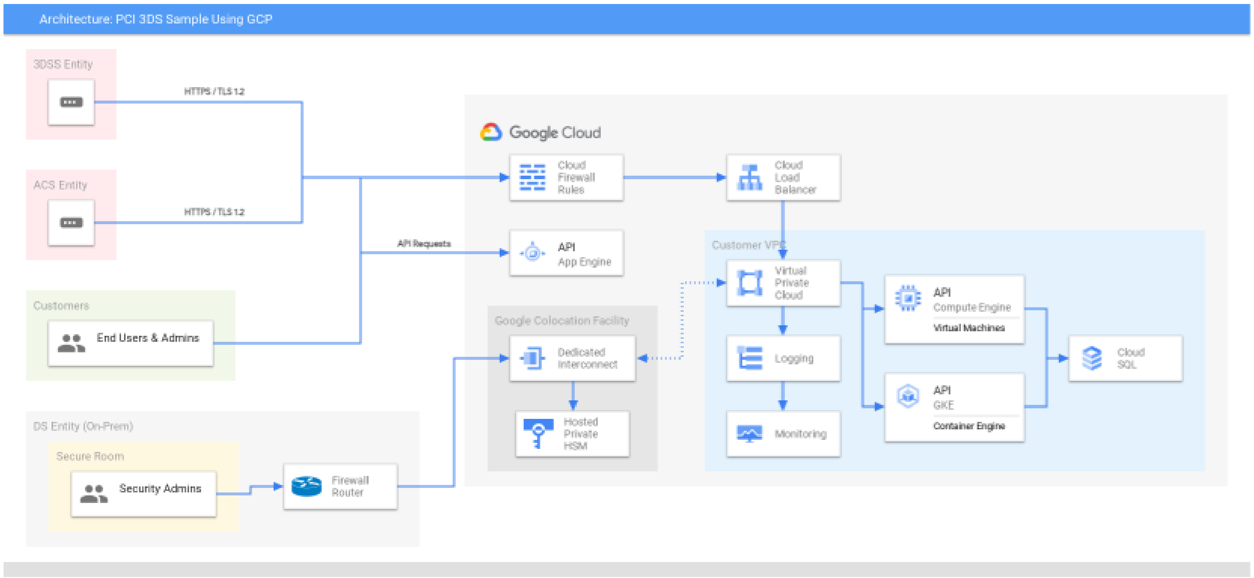


Figure 4: Sample 3DS Architecture Diagram

Figure 4 shows a sample high-level architecture diagram, and the description noted below demonstrates implementation of a 3DS DS component in Google Cloud using various products. Google Cloud customers share responsibilities when configuring products for their PCI DSS or PCI 3DS needs.

- The 3DSS entity and ACS entity act as the external components where messages are routed by the DS service.
- Google Cloud customers (end-users) log in to GFE using configured MFA controls.
- The DS entity on-premises network consists of a secure room with logical and physical controls implemented per the 3DS requirements. This secure room may potentially consist of an HSM or non-console access systems for accessing the HSMs within the Google colocation facility for managing the HSM as per the logical and physical security characteristics identified within 3DS control.
- A Cloud SQL database contains the encrypted 3DS authentication data and utilizes the BYOHSM for management of cryptographic keys.
- The DS servers (virtual machines) are hosted in Compute Engine.
- GKE is used for deploying containerized applications.
- The 3DS messages are handled through Cloud Load Balancer.
- Google Cloud's VPC service provides the capability to secure the perimeter and constrain data.
- Logging and monitoring controls are configured at the product level, and logs are exported to BigQuery for analysis.

CONCLUSION

Coalfire conducted a PCI 3DS assessment for Google Cloud and validated it against the PCI 3DS Core Security Standard. A PCI 3DS AOC is available from the Google Compliance team. Google maintains and manages its own compliance for the PCI 3DS Core Security Standard as part of its service provider responsibilities. Based on the PCI 3DS assessment validation, Coalfire determined that Google Cloud PCI 3DS service provider environment meets the applicable PCI 3DS controls. 3DS entities that utilize Google products must understand their responsibilities and be aware of the in-scope services that must be maintained and configured per the guidance from Google for the PCI 3DS environment to be compliant. 3DS entities will also have responsibilities to meet the PCI 3DS Core Security Standard requirements that are not met directly using Google Cloud products.

Coalfire expressly disclaims all liability with respect to actions taken or not taken based on the contents of this assessment.

RESOURCES

The following sources provide additional information and guidance related to this document:

- PCI 3DS Requirements:
  https://www.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss
- PCI DSS 3.2.1 Requirements:
  https://www.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss
- PCI 3DS Data Matrix:
  https://www.pcisecuritystandards.org/documents/PCI-3DS-Data-Matrix-v1_1.pdf
- EMVCo 3DS Specification
  https://www.emvco.com/terms-of-use/?u=/wp-content/uploads/documents/EMVCo_3DS_Spec_v220_122018.pdf
- Google Compliance – PCI DSS:
  https://cloud.google.com/architecture/pci-dss-compliance-in-gcp
- Google Products Security Documentation:
  - Security Design Whitepaper: https://cloud.google.com/security/infrastructure/design
  - Security Whitepaper: https://cloud.google.com/security/overview/whitepaper

ABOUT THE AUTHOR

Bhavna Sondhi | Principal

Bhavna Sondhi is the practice subject matter expert for the solution validation team at Coalfire. Bhavna performs advisory work and assessments for various PCI compliance frameworks and authors technical white papers. Bhavna joined Coalfire in 2013 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 the teams recognize the importance of secure code development and information security within their operational practices.

ABOUT THE REVIEWER

Andrew Barratt | Managing Principal

Andrew Barratt leads several global service lines at Coalfire. With expertise in the financial services industry and the payment processing community, he brings over 20 years of experience in IT and security. He maintains the QSA, PA-QSA, 3DS, P2PE, PA-P2PE, and Core PFI-investigator credentials to help support clients around the world with some of their most complex security and compliance challenges.

Published 27 July 2021.

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 nearly 20 years and has offices throughout the United States and Europe. For more information, visit Coalfire.com.

Coalfire is solely responsible for the contents of this document as of the date of publication. The contents of this document are subject to change at any time based on revisions to the applicable regulations and standards (HIPAA, PCI DSS et.al). Consequently, any forward-looking statements are not predictions and are subject to change without notice. While Coalfire has endeavored to ensure that the information contained in this document has been obtained from reliable sources, there may be regulatory, compliance, or other reasons that prevent us from doing so. Consequently, Coalfire is not responsible for any errors or omissions, or for the results obtained from the use of this information. Coalfire reserves the right to revise any or all of this document to reflect an accurate representation of the content relative to the current technology landscape. In order to maintain contextual accuracy of this document, all references to this document must explicitly reference the entirety of the document inclusive of the title and publication date; neither party will publish a press release referring to the other party or excerpting highlights from the document without prior written approval of the other party. If you have questions with regard to any legal or compliance matters referenced herein you should consult legal counsel, your security advisor and/or your relevant standard authority.

Google Cloud Platform for PCI 3DS, July 2021