COALFIRE

WHITE PAPER

Google Cloud for PCI 3DS

BHAVNA SONDHI | CISA, ISO/IEC 27001 LEAD IMPLEMENTER, CEH, 3DSA, QPA, P2PE ASSESSOR, P2PE APPLICATION ASSESSOR, SECURE SOFTWARE ASSESSOR, SECURE SLC ASSESSOR

SAM PFANSTIEL, PH.D. | CISSP, CISM, CISA, CEH, 3DSA, QPA, P2PE ASSESSOR, SECURE SOFTWARE ASSESSOR, SECURE SLC ASSESSOR

Google Cloud

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 3-D Secure (3DS) assessor company, to conduct an assessment of Google Cloud (formerly referred to as Google Cloud Platform [GCP]) against the PCI 3DS Core Security Standard v1.0 (“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 from 1 Feb 2022, to 24 June 2022. An Attestation of Compliance (AOC) document for the assessed PCI 3DS environment was provided to the Google compliance team on 6 July 2022. Coalfire determined that Google Cloud does not operate a distinct PCI 3-D Secure Environment (3DE) but provides services which may be subsequently used within a Google Cloud customer’s 3DE.

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 a 3DS solution. All products evaluated during the assessment, and discussed further herein, are therefore subject to compliance impacts based on customer implementation.

The goal of this white paper is to provide guidance to customers for hosting their PCI 3DE within 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 3DS Solution, or any portion thereof, in Google Cloud.

This paper provides an overview of the 3DS domains, examines the relationship between the PCI Data Security Standard (DSS) and PCI 3DS Core Security Standard, and defines the responsibilities shared by Google Cloud and its customers to meet the PCI 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?

While “3DS Core” is a security standard and assessment program defined and managed by the PCI Security Standards Council, “3DS” is a specification defined and managed by EMVCo (eponymously named for its founding members, Europay, Mastercard, and Visa). Based on an Extensible Markup Language (XML) messaging protocol, 3DS enables cardholders to authenticate 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 to detect and reduce fraudulent transactions. 3DS is defined within the EMV® 3-D Secure Protocol and Core Functions Specification (EMV 3DS Specification).

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 requestor environment (which may include the 3DS client, 3DS requestor interfaces, and the 3DS Server [3DSS]), the 3DS integrator, and the acquirer.

[1] https://www.emvco.com/wp-content/uploads/documents/EMVCo_3DS_CoreSpec_v2.3.1_20220831.pdf

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

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

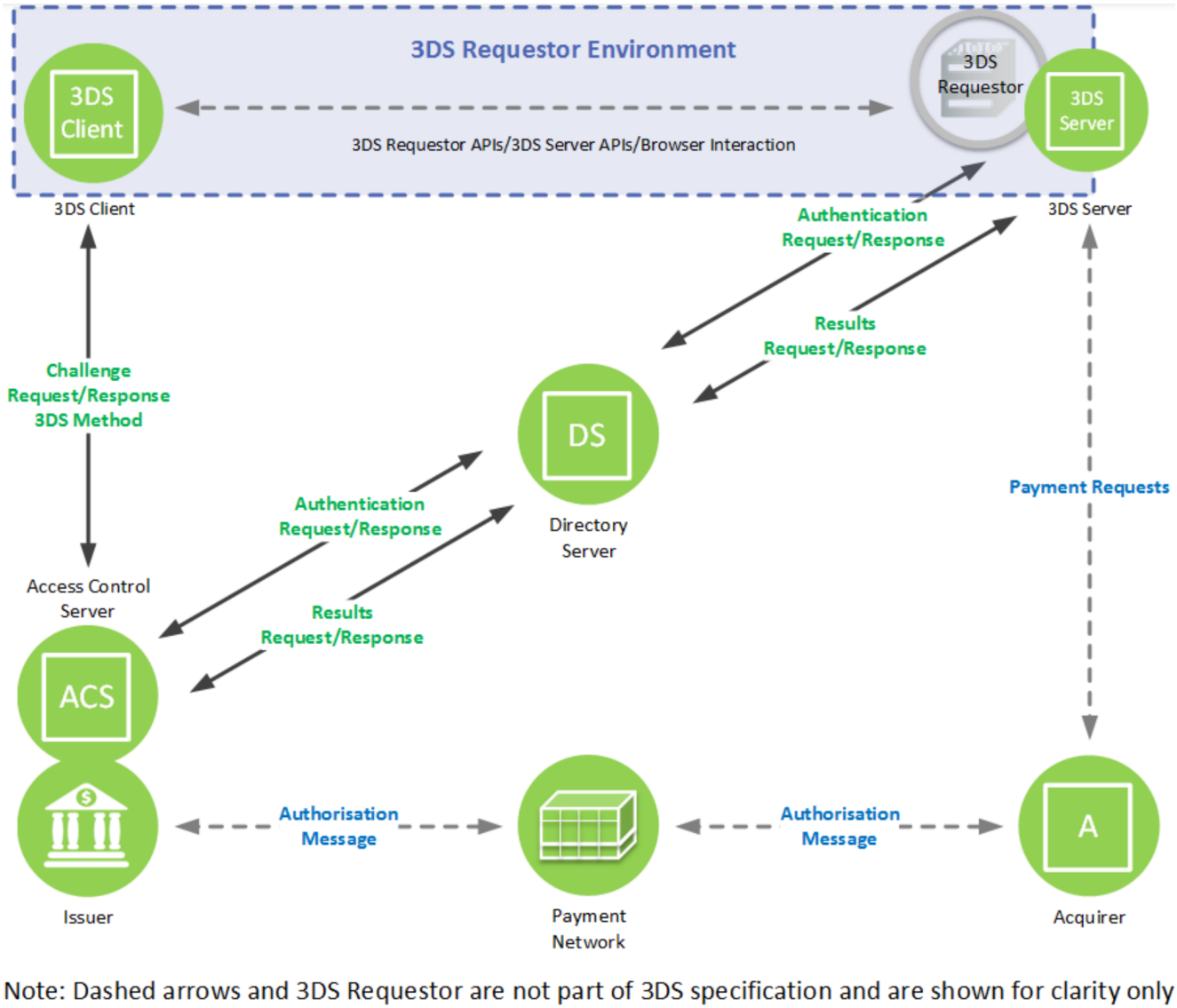

Figure 1: 3DS Domains and Components[2]

[2] https://www.emvco.com/wp-content/uploads/documents/EMVCo_3DS_CoreSpec_v2.3.1_20220831.pdf

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 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:
  - Verifying whether 3DS authentication is available for a particular card number.
  - Authenticating the specific cardholder for the transaction once a card is validated as eligible for the transaction.
  - Sending a response back to the requestor environment after the cardholder is validated and approved.

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

- **3DS ACS**: Contains the authentication rules and is managed within the issuer domain.
- **3DSS**: Provides the functional interface between the 3DS requestor 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.

3DS Third-Party Service Provider 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 within the context of the customer's 3DS solution. Other components that make up a customer's 3DE include network devices, servers, applications, and computing devices.

PCI 3DS Core Security Standard 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 which may be used within the customer's 3DE. Therefore, while Google Cloud does not itself provide a 3DS solution, it is eligible to be validated as a third-party service provider for the applicable PCI 3DS Core Security Standard requirements. Google Cloud products may be utilized by 3DS customers to host all or part of their 3DE, as well as to provide security controls for those systems. 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.

PCI DSS and PCI 3DS Core Security Standard

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

Google Cloud offers products, a selection of which are outlined in Appendix A, that may be used to support customers' solutions for 3DS functions. Google Cloud does not perform the functions of 3DSS, DS, or ACS 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 PCI 3DS Combined Environments. The PCI 3DS Standalone Environment applies to customers who are not required to be assessed under PCI DSS but are eligible to be validated under PCI 3DS Core Security Standard; these environments must be assessed to both Part 1 and Part 2 of PCI 3DS Core.

In both cases, responsibilities for meeting the applicable controls are shared between Google Cloud and the customer.

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

- **Part 1: Baseline Security Requirements**: Technical and operational security requirements designed to protect the 3DE, the substance of which may also be found in the PCI DSS standard.
- **Part 2: 3DS Security Requirements**: Security requirements designed specifically to protect 3DS data and processes. These controls are above and beyond those found in the PCI DSS standard.

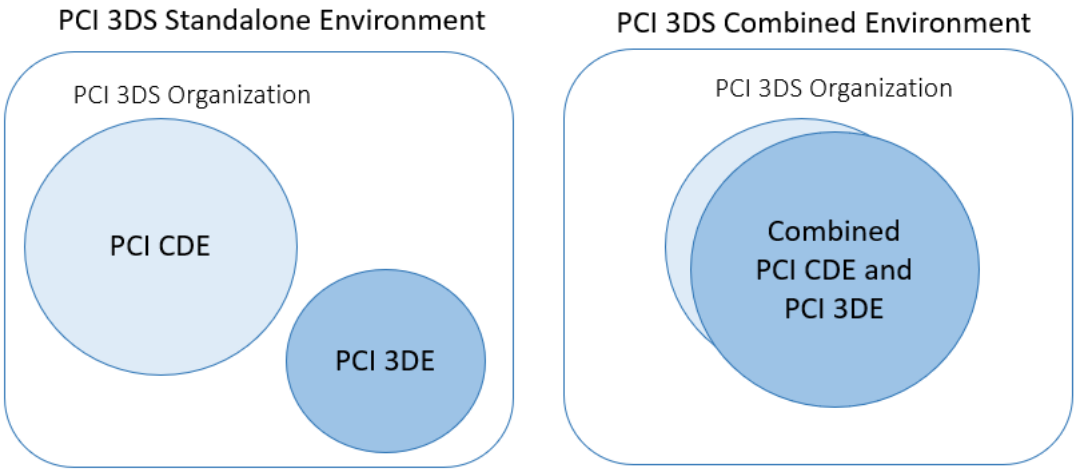

Figure 2: 3DE Scenarios

PCI 3DS Overview for Google Customers

Within each of the following subsections, the individual controls of the PCI 3DS Core Security Standard are discussed in relation to Google Cloud's architecture, including descriptions of the responsibilities that Google Cloud assumes for its products and the customer's responsibilities when utilizing the in-scope Google Cloud products. Further details on shared responsibilities, as they pertain to specific PCI 3DS Core Security Standard requirements, may be viewed in Appendix B.

PCI 3DS Part 1: Baseline Security Requirements

As Google Cloud is hosted within its own 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 PCI 3DS Core Security Standard 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 to the respective PCI security frameworks.
- **Google Cloud PCI DSS and PCI 3DS Responsibility Matrix**: The shared responsibility matrices identify the responsibilities shared between Google Cloud and its customers for the respective PCI security frameworks.
- **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, and PCI 3DS Core Security Standard requirement P2-2.4, customers must maintain written agreements with third-party service providers and implement a program to monitor service providers' compliance status at least annually.
- **Product Implementation Guidance**: Google Cloud customers should identify the in-scope products and ensure that they are implemented and configured in accordance with Google Cloud guidelines and are in compliance with PCI DSS requirements.

PCI 3DS Part 2: Security Requirements to Protect 3DS Data and Processes

Google Cloud's 3DS environment meets the applicable requirements identified within PCI 3DS Core Security Standard Part 2, as demonstrated in the PCI 3DS AOC dated July 6, 2022, 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 all applicable controls:

- **Google Cloud PCI 3DS Responsibility Matrix**: This document outlines the in-scope Google Cloud products that can be used to meet PCI 3DS Core Security Standard Part 2 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 sections below provide high-level guidance for the PCI 3DS requirements in PCI 3DS Core Security Standard Part 2 and how Google Cloud products can assist with achieving compliance for environments hosted in Google Cloud. This guidance is not a turnkey solution; specific configurations must be performed by the customer utilizing Google Cloud for hosting their PCI 3DS environment. Example reference architectures may also be found in Appendix C.

Requirement P2-1: Validate Scope

In addition to identification of 3DE system components (P2-1.1.1), segmentation is recommended to limit the scope for the PCI DSS and PCI 3DS environment (P2-1.1.2). The PCI 3DE can be part of the PCI DSS cardholder data environment (CDE) or segmented from the entity's network to achieve further 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.

Technical controls for segmentation for Google Cloud may consist of one or more of the following means:

- Logical segmentation using Resource Manager to enforce resource hierarchy
- Network segmentation using Virtual Private Clouds (VPCs), subnets, and firewall rules and policies
- Service level segmentation using VPC Service Controls
- Further segmentation may be performed for containers using Google Kubernetes Engine (GKE) by utilizing namespaces and network policies to partition workloads between clusters and using Private Clusters for non-public nodes and pods.

In addition to network and system scope delineation, access to all 3DE resources must be tightly controlled (P2-1.1.3). Use of IAM roles is recommended to ensure users with access to 3DE resources are easily managed and are reviewed periodically.

Requirement P2-2: Security Governance

Security governance programs should identify and define the security objectives (P2-2.1.1), roles and responsibilities (P2-2.1.2, P2-2.1.3), risk management strategy (P2-2.2.1, P2-2.2.2), and management of third-party relationships specific to the 3DE (P2-2.4). Reviewing and monitoring of procedures for detecting and responding to security control failures must also be implemented (P2-2.3).

Google recommends the following best practices to define access policies and implement strong access controls:

- IAM with role-based access controls (RBACs) provides granular access to 3DE resources.
- Access for administrative tasks is granted via IAM and then revoked upon completion of the task.
- Cloud Identity provides multi-factor authentication (MFA); OTP, and certificate-based authentication.

Requirement P2-3: Protect 3DS Systems and Applications

Protect boundaries (P2-3.1)

Traffic between 3DS components must be protected and permitted for purposes of 3DS transactions or to support 3DS functions, such as security or management. All interfaces, including physical, logical, and virtual, must be identified and protected against both network layer attacks.

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

- Configure firewall rules to protect access to Compute Engine VM instances and GKE cluster nodes.
- Configure network policies to restrict flows in and between GKE cluster pods and services.

Protect baseline configurations (P2-2.2)

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.

The following controls for 3DS data and files should be considered to protect the application baseline configuration and secure application interfaces:

- Follow the principle of least privilege for access to sensitive application code and service configuration in Google Cloud, using IAM for authorization with granular access permissions configured using RBAC.
- Google Cloud provides the following guidelines for deploying workloads on GKE clusters that align with PCI DSS, which is also useful for 3DS architecture considerations:
  - Use configuration management for Kubernetes to require strict control of pod images, sets, and templates. Google recommends use of Autopilot, which enforces security best practices for initial configuration.
  - Create private GKE clusters where nodes only have internal IP addresses, isolating the nodes and pods from the internet.
  - Protect nodes, containers, and pods and secure those components in GKE. (Kubernetes control plane components are managed by Google.)
  - GKE deploys workloads on Compute Engine instances within Google Cloud. These instances are attached to the GKE cluster as nodes. Use controls identified within the GKE guides to achieve node-level security protection.
  - Use the shielded GKE nodes feature, which provides verifiable node identity and integrity to increase the security of GKE nodes.
- Terraform Config Validator, while not generally available (GA), may be used to define constraints for enforcing security and governance policies for use of infrastructure-as-code resources in the 3DE.

Protect applications and application interfaces (P2-3.3)

Applications and application interfaces must be monitored (P2-3.3.2) and protected (P2-3.3.1) from unauthorized changes in production, and all APIs must be identified (P2-3.3.3) and controlled (P2-3.3.4)

Google tools which support the protection of production applications and APIs include:

- Load Balancer: Provides traffic filtering, which may be used to protect application web interfaces and API.
- Apigee: Supports the identification and monitoring of approved remote APIs that interface with the 3DE.

Applications and APIs deployed using GKE can be protected using the following approaches:

- 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

- For GKE workloads, communication traffic with other services running inside or outside the cluster should be controlled. This can be achieved by use of network policies to limiting pod-to-pod communication as well as outside communications.

Secure web configurations (P2-3.4)

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 recommends the following to secure web configurations:

- To enforce HTTPS for inbound communications, or restrict access based on required HTTP header information, use of HTTPS Load Balancer is recommended.
- Entities may use Cloud Armor to protect applications from a variety of application layer attacks, including OWASP Top 10 vulnerabilities.
- Cloud Data Loss Prevention can be used to prevent disclosure of 3DS data via insecure outbound channels.
- When utilizing GKE, customers can define ingress rules for enforcing HTTPS traffic to applications running in the cluster.

Maintain availability of 3DS operations (P2-3.5)

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 recommends the following to maintain the availability of 3DS operations:

- Demand forecasting to anticipate future load is important to allocate sufficient compute resources for 3DS services. Google Cloud's guidance for managing capacity includes reviewing utilization via Console, CLI, or BigQuery API; creating forecasting models; and using Cloud Monitor to track usage.
- Google Cloud Compute Engine high availability features, such as availability regions and zones, managed instance groups (MIGs), autoscaling, autohealing, and load balancing, can be used to ensure high availability of the 3DS application, per PCI 3DS requirements.
- 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 application resource usage for high availability.
- Cloud Armor provides edge protection from threats to availability, including distributed denial-of-service (DDoS).
- Cloud Monitoring uses log-based metrics to provide alerting in the event of missed service level indicators (SLI), objectives (SLO), or agreements (SLA).

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

The sections below outline scenarios that are included in the requirement to secure connections to the 3DS solution.

Secure connections for issuer and merchant customers (P2-4.1)

Where the 3DS entity provides issuer and merchant users with access to 3DS services, these connections require unique user ID with strong password and another form of strong authentication. It is the responsibility of customers to configure their applications to meet this requirement, however Google does offer the Identity Platform, which may be used to incorporate authentication into customer applications built on App Engine or otherwise using Google Cloud application interfaces.

Secure internal network connections (P2-4.2) and Secure remote access (P2-4.3)

Any non-console access to 3DS components (ACS, DS, or 3DSS) must originate from the entity's network and must utilize MFA applied at the network, system, or application level. Also called Two-Step Verification (2SV), MFA requires entities to authenticate using at least two different factors. The three available factors are "something you know" (e.g., a password or passphrase), "something you have" (e.g., a smartphone or token), and "something you are" (e.g., a fingerprint or facial recognition). MFA may be implemented using one or more of the following Google services:

- Cloud Identity supports use of Titan security keys, SMS, phone call, or smartphone authenticator application.
- BeyondCorp Enterprise is a zero-trust authentication model that 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 under two-step verification.
- Identity Platform is an API and SDK that allows customers to integrate in-application authentication into their applications and includes multi-factor options.

Restrict wireless exposure (P2-4.4)

Wireless connections for 3DS components are prohibited (P2-4.4); however, Google Cloud offers no such capability and uses no wireless within its production data centers. Therefore, this control is not applicable for customers whose 3DEs reside entirely within Google Cloud.

Secure VPNs (P2-4.5)

All virtual private network (VPN) access to the 3DE should be reviewed against industry-recommended implementations. Note that Google does not use a VPN to access its production networks but does offer Google Cloud VPN for customers who wish to provide such access to its own environment. Google Cloud VPN provides strong encryption of communications between VPCs, between applications, or over public networks using IPSec, and protects against eavesdropping, replay, or man-in-the-middle attacks.

Requirement P2-5: Protect 3DS Data

Data lifecycle, retention, and data storage (P2-5.1)

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

Google offers several storage options for applications, such as Cloud SQL, data storage, or Cloud Spanner. When utilizing cloud storage options, refer to the best practice guidance from Google Cloud, as well as to the PCI 3DS data matrix, to

ensure that the Google Cloud storage options utilized store only the data types permitted by PCI 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. When addressing this standard, Google Cloud customers should also consider:

- Evaluating the sensitivity and protection of data based on their risk-management policy and configure the applications developed or the Google Cloud products utilized accordingly.
- Leveraging Compute Engine options, such as persistent disk, local storage, cloud storage buckets.
- Using encryption, truncation, masking, and hashing in Google Cloud Storage buckets, BigQuery instances, Datastore, Cloud SQL, and Cloud Spanner to protect sensitive data at rest.

Data transmission (P2-5.2)

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 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:

- Load Balancer provides protocol restrictions and enforces HTTPS / TLS version and cipher suites for user-to-GFE, service-to-service, and VM-to-VM transmissions.
- Transmissions from customer on-premises data centers may be protected to Google Cloud using Private Service Connect.

When configuring TLS communications between ACS, DS, and 3DSS components, TLS v1.2 or higher is required, and the below ciphers 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 permitted or supported in 3DS environments:

- Any cipher suite represented as “Null” or “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”
- Any cipher suite incorporating 3DES and SHA-1 (these 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 EMV 3DS Specification for additional details.

Monitor 3DS transactions (P2-5.2)

Customers are responsible for monitoring 3DS transactions to detect anomalies and generate logs and alerts. Monitoring can be enabled for various Google Cloud products. See below for an example of product monitoring features:

- Cloud SQL
- Dataflow
- Dataproc
- GCS
- Cloud Key Management Service (KMS)
- Pub/Sub
- Cloud Functions

Requirement P2-6: Cryptography and Key Management

Key management (P2-6.1)

The 3DS entities' policies should cover all cryptographic keys and processes used for protecting the 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 the 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, and 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. Cloud KMS and/or Secret Manager may also be used to accommodate the protections for 3DS sensitive data. Consult the 3DS Data Matrix for more information.

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 lifecycle of key management, as well as for 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. Customers can use a cloud-based HSM for 3DSS environments but should evaluate the feasibility of products for use in an ACS and DS environment.

Secure logical access to HSMs (P2-6.2)

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.

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 from many options to satisfy the stringent requirements for HSMs that manage in-scope 3DS ACS and DS keys. Below, four options are discussed for utilizing HSM: Cloud HSM, External HSM, Marketplace HSM Solutions, or Hosted Private HSM.

- **Cloud HSM**
  - Cloud HSM utilizes FIPS 140-2 Level 3 (overall) approved HSM with all FIPS-approved configurations. Google uses console access to manage the Cloud HSM and root keys (P2-6.1.1-4). The customer is responsible for its own customer-managed encryption key (CMEK) hierarchy and all key management in accordance with applicable 3DS requirements in PCI 3DS Core Security Standard Part 2, control objective 6.
  - Non-console access solutions require evaluation by an independent laboratory in accordance with sections of International Organization for Standardization (ISO) 13491 identified within the PCI 3DS Core Security Standard (P2-6.2.1). Cloud HSM has not been evaluated to the applicable modules of ISO 13491 to support HSM non-console access. Similarly, PCI 3DS Core Security Standard 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. Therefore, the customer is ultimately responsible for administration of these systems without utilizing non-console access or clear-text keys or for implementation of appropriate compensating controls if non-console access is required.
- **External HSM**
  - A 3DS entity may wish to host their FIPS 140-2 Level 3 or PCT PTS-approved HSM in a non-Google Cloud environment (such as their own data center or other on-premises network) that meets all 3DS requirements for HSMs. In such cases, Google Cloud Interconnect may provide a secure, dedicated connection from the VPC to the customer's off-cloud network, as shown in Figure 3 below.

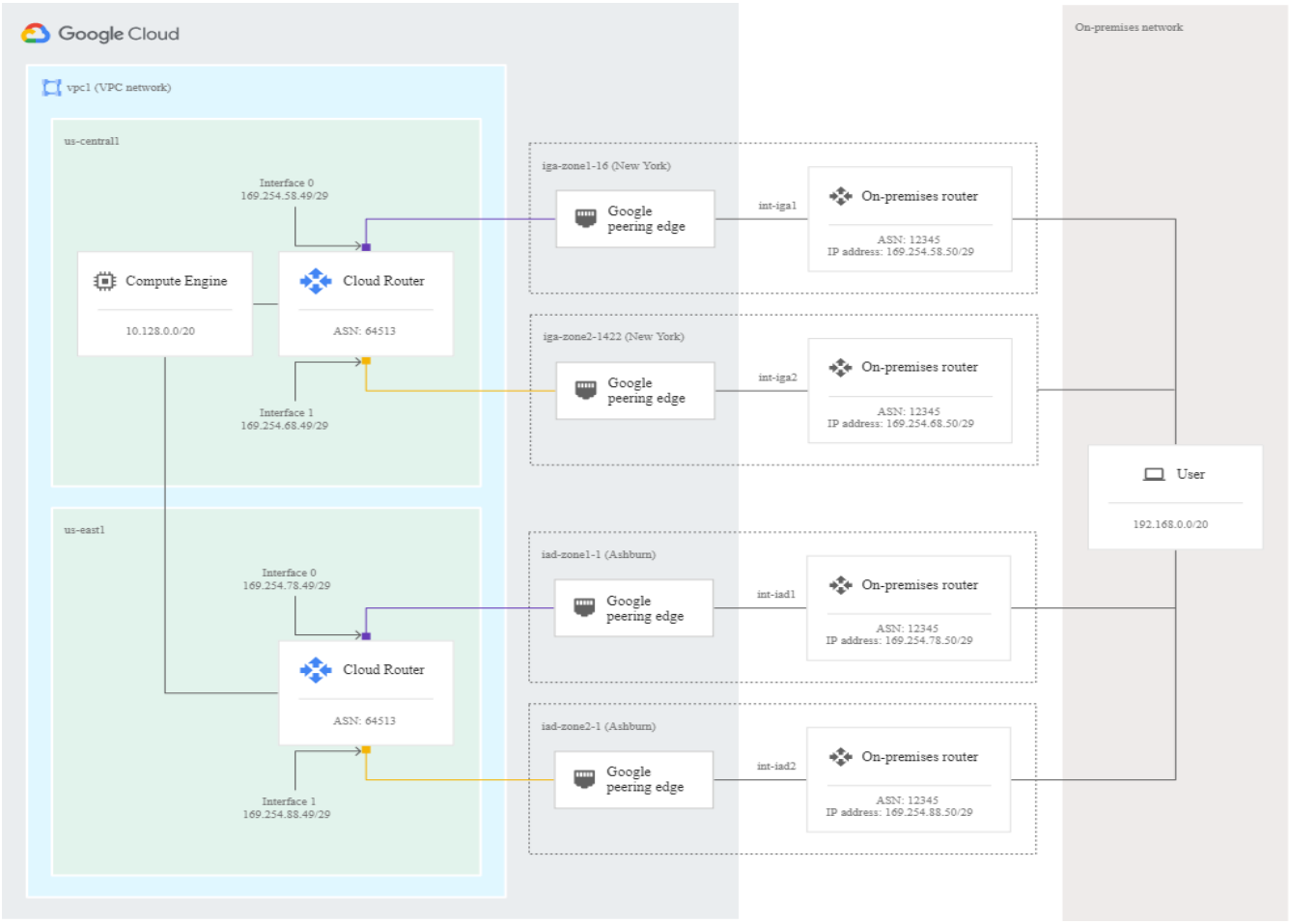

Figure 3: Google Cloud Interconnect Architecture

- **Marketplace HSM Solutions**
  - The Google Cloud Marketplace is a growing community of SaaS applications and services which may integrate quickly and seamlessly with Google native products. Due to constant updates to available third-party solutions within the marketplace, no HSM third-party marketplace vendors were evaluated for this white paper.
  - 3DS customers who must meet the HSM requirements of the 3DS standard but do not wish to use Cloud HSM or host their own HSMs are encouraged to evaluate the available options within the Google Cloud Marketplace for suitability for their solution and the ability to meet all applicable 3DS controls. As with all options presented here, the ultimate responsibility for 3DS compliance falls to the customer.
- **Hosted Private HSM**
  - Certain customers may be eligible for use of Google Cloud Hosted Private HSM. While not an option for all Google customers, this service allows for deployment of customer-owned HSMs within Google's colocation facility.
  - Customers using Hosted Private HSM should ensure they configure the HSMs per PTS or FIPS security policy, including HSM provisioning 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 applicable modules of the current version of ISO 13491, per P2-6.2.1.
- 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

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 capture footage at all times of the day and night is required for monitoring entry and exit points.

All P2-7 physical security controls have been confirmed as in place for the Google Cloud 3DE. For any 3DS components not hosted in the Google Cloud (e.g., external HSM via Cloud Interconnect; remote administration network), customers are responsible for managing 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 the data center environment.

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 the 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.

Appendix A – Google Cloud 3DS Products

The following products are provided by Google Cloud to customers to support their PCI 3DS environments, as discussed in the body of this document.

Google Cloud Product	Description	Documentation
Cloud KMS	Cloud KMS is a cloud-hosted, key management service that lets customers manage cryptographic keys for their cloud services the same way they do on premises. Customers can generate, use, rotate, and destroy AES-256, 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
Cloud HSM	Cloud HSM is a cloud-hosted, key management service that utilizes FIPS 140-2 Level 3 HSMs to protect encryption keys and perform cryptographic operations within a managed HSM service. Customers can generate, use, rotate, and destroy various symmetric and asymmetric keys.	https://cloud.google.com/kms/docs/hsm
Cloud Armor	Cloud Armor protects edge services through use of adaptive protection and learning. Features include protection against OWASP attacks (P2-3.3.4), protection against unauthorized embedding of links within pages, and geography-specific rules providing varying domain protection based on customer risk profiles (P2-3.3.3). Google recommends running Cloud Armor in Autopilot mode, since most 3DS applications are not stateful.	https://cloud.google.com/armor
Google Cloud VPC	The shared VPC model provides granular control for network administrators around policies and rules that are compliant across the customer organization.	https://cloud.google.com/vpc
Google Kubernetes Engine	GKE, powered by the open-source container scheduler Kubernetes, enables customers to run containers on Google Cloud. GKE provisions and maintains the underlying virtual machine cluster, scaling a customer's application, and manages operational logistics such as logging, monitoring, and cluster health management. The Kubernetes cluster architecture can also enable identity management, preventing running of service from unauthorized sources, and Dataflow Prime restricts which services can call other services (P2-3.4.3, P2-3.4.4). GKE also allows restriction of access to certain TLS versions , defaulting to 1.2. The customer is responsible for identifying and addressing vulnerabilities, but container vulnerability scanning supports detection of common CVE.	https://cloud.google.com/kubernetes-engine/docs/how-to
Container Analysis	Container-level security may be configured via the Container Analysis APIs or client libraries. This product allows for scanning for OS- or package-level vulnerabilities, aiding in vulnerability detection and response.	https://cloud.google.com/container-analysis/docs/on-demand-scanning-howto https://cloud.google.com/container-analysis/docs/automated-scanning-howto

Google Cloud Product	Description	Documentation
BeyondCorp Enterprise (BCE)	Google provides strong communications and protects against eavesdropping, replay, or man-in-the-middle attacks using the BeyondCorp zero-trust model. BCE 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.	https://cloud.google.com/identity-platform/docs/web/mfa https://cloud.google.com/beyondcorp-enterprise
VPN	Where VPN is required for remote access, Google Classic and High Availability VPN services support remote access to cloud resources using IPSec, strong cryptography, and secure authentication, preventing common threats such as eavesdropping and man-in the-middle attacks (P2-4.5).	https://cloud.google.com/network-connectivity/docs/vpn/concepts/overview
Private Service Connect	Private Service Connect allows private consumption of services across VPC networks that belong to different groups, teams, projects, or organizations. Connections may be made to authorized external resources using customer-defined IP addresses, allowing them to operate as internal systems within the VPC network.	https://cloud.google.com/vpc/docs/private-service-connect
Apigee	Apigee is an embedded API management system, API gateway, and abstraction layer for external interfaces. This service simplifies connections to multiple acquiring banks, for instance, as well as aids in enumeration of authorized API remote endpoints (P2-3.3.3). Security features include rate limiting, which can serve as a risk-based approach to reducing unauthorized connections and enforcing HTTPS connections (P2-3.4.2). Apigee includes OWASP protections to protect APIs against common attacks, including CSRF and injection (P2-3.4.5).	https://cloud.google.com/apigee
Secret Manager	Secret Manager layers on top of Cloud KMS to secure store API keys, passwords, and certificates. Cloud KMS supports stronger controls for protection of authentication and customer-managed encryption keys (CMEK),where an HSM is not required.	https://cloud.google.com/secret-manager
Monitoring	Application health monitoring ensures availability, in accordance with P2-3.5.2.	https://cloud.google.com/monitoring
Logging	Google Logging and Audit Logging may be used to meet requirements for other Google Cloud products (P2-5.3.4, P2-5.5.2, P2-6.1.9).	https://cloud.google.com/logging https://cloud.google.com/audit-logs
Google Workspace	Formerly G Suite, Google Workspace provides additional levels of enterprise protection that may be used to satisfy security controls, such as restricting access based on time of day or location.	https://workspace.google.com/security/
Google Compute Engine (GCE)	GCE offers scalable and flexible virtual machine computing capabilities in the cloud, with options to utilize certain CPUs, GPUs, or Cloud TPUs. Customers can use GCE to solve large-scale processing and analytic problems on	https://cloud.google.com/compute/docs/how-to

Google Cloud Product	Description	Documentation
	Google's computing, storage, and networking infrastructure.	
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 customers to create, configure, and use relational databases that live in Google's cloud. It is a fully managed service that maintains, manages, and administers customer databases, including high-availability configurations (P2-3).	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
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 lifecycle of GCE 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, customers can create Spark/Hadoop clusters sized for their workloads as needed.	https://cloud.google.com/dataproc/docs/how-to
Google Cloud Storage	Google Cloud Storage is a RESTful service for storing and accessing customer 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	https://cloud.google.com/kms/docs/hosted-private-hsm

Google Cloud Product	Description	Documentation
	certified HSMs and is not a generalized hosting or colocation service.	
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
Cloud Functions	Cloud Functions is a lightweight, event-based, asynchronous compute solution that allows customers 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 Products

Appendix B – Shared Responsibilities

The PCI 3DS Core Security Standard program allows for entities to meet control requirements by use of third-party service providers (TPSPs), such as Google Cloud. 3DS entities, however, are responsible for documenting and understanding how each of these controls may be met by entirely the TPSP, by the customer alone, or—as is often the case—through a sharing of responsibilities. Google Cloud customers to who wish to leverage the Google Cloud 3DS assessment to reduce the effort required for 3DS validation must fully understand how each product and control relies upon the clear communication of shared responsibilities.

Google Cloud has been assessed to demonstrate that a complaint PCI DSS Report on Compliance (ROC) is in place to satisfy Part 1 controls, and that all access by Google personnel is performed in a compliant manner, and that physical security controls are in place. However, where any Google products are relied upon to meet 3DS requirements, it is the responsibility of the customer to ensure that all in-scope products hosted in Google Cloud are configured and managed to ensure their compliance to applicable 3DS security controls. 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 HSM products or co-location services aimed at meeting the requirements for FIPS 140-2 Level 3 HSMs hosted within physically secure data centers, thereby meeting the common PCI 3DS requirements applicable to all ACS, DS, and 3DSS environments. Specific controls related to HSM logical access and key management for ACS and DS environments must be reviewed by the customer to ensure they meet requirements based on the customer implementation.
- Google Cloud protects infrastructure, including hardware and software; however, customers are required to implement and configure the products as per the 3DS requirements.

The high-level 3DS Requirements, PCI DSS corresponding requirements, and the responsibilities of Google Cloud and Google Cloud customers are outlined at a high level below. Please refer to Google Cloud Platform's Shared Responsibility Matrix for additional information, which is available upon request from the Google Compliance team:

3DS Requirement		Responsibility Summary	
		Google Cloud	Customer
P1	3DS Core Part 1 (all sections)	Google Cloud is responsible for conducting annual PCI DSS and PCI 3DS assessments, thereby satisfying its Part 1 compliance responsibilities as a 3DS third-party service provider.	Google Cloud customers are responsible for implementing their own 3DS environment in accordance with the 3DS program. • If implemented within a PCI DSS CDE, Part 1 may not be applicable for the customer. The customer should leverage the Google Cloud PCI DSS AOC and PCI DSS responsibility summary documentation (which may also be obtained from the Google Compliance team) as part of their PCI DSS

3DS Requirement			Responsibility Summary	
			Google Cloud	Customer
				assessment, then complete PCI 3DS section 2.3, as applicable to the customer 3DE. • If the customer 3DE does not reside within a PCI DSS CDE, the customer is fully responsible to meet all Part 1 requirements. The Google Cloud PCI DSS AOC and PCI 3DS AOC may be used to satisfy evidence requirements for these controls.
P2-1	Validate scope	1.1 Scoping	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 a customer's 3DE. The Google Cloud environment includes infrastructure, development, operations, management, support, and the in-scope products.	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 meets the applicable controls for its environment as identified within the PCI 3DS AOC.	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 3.4 Secure web configurations 3.5 Maintain availability of 3DS operations	Google Cloud meets the applicable controls for its environment as identified within the PCI 3DS AOC. Controls specific to managing traffic between 3DS components is the responsibility of the customer. More information on Google Cloud security design is available here: • Google Cloud Security Design Whitepaper • Google Cloud Security Whitepaper	Google Cloud customers are responsible for implementing the in-scope products per Google Cloud guidelines to meet the PCI 3DS controls. Documentation to assist customers in securing all Google Cloud product configuration baselines may be obtained within the documentation for the respective products. Documentation to assist customers in configuring high availability 3DS operations may be obtained region and zone documentation.

3DS Requirement			Responsibility Summary	
			Google Cloud	Customer
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 meets the applicable controls for securing access by Google personnel to the Google Cloud environment, as identified within the PCI 3DS AOC.	Customers are responsible for configuring logical access to all in-scope products for their 3DE.
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 meets the applicable controls for their environment as identified within the PCI 3DS AOC.	Customers are responsible for configuring the in-scope products and for protecting the 3DS data within their 3DE. For configuration guidance, see the Google Cloud 3DS Products section and the Google Cloud security baseline documentation.
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 offers products such as Cloud KMS and Cloud HSM key management for 3DSS. Google Cloud meets the controls applicable for their environment.	Google Cloud customers are responsible for managing all cryptographic key management processes for their own 3DS solution. **3DSS solutions:** Customers may also utilize Cloud HSM, Cloud KMS, or Secret Manager for key management processes to protect sensitive 3DS data. **ACS and DS solutions:** Customers are responsible for meeting HSM requirements to accommodate their key loading and remote access requirements. ACS and DS customers are responsible for configuration of the HSMs per PTS or FIPS security policy, including the HSM provisioning and securing logical access to HSMs for ACS and the DS 3DS environment as identified within the 3DS requirement. Similarly, it is the customer's responsibility to utilize non-console access to the HSM that complies with the current version of ISO-13491.
P2-7	Physically secure 3DS systems	7.1 Data center security 7.2 CCTV	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.	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 MFA controls into telecommunications rooms hosted in their 3DE, as applicable.

Table 2: Google Cloud PCI 3DS Requirements Responsibility

Appendix C – Reference Architectures

Two reference architectures are provided to assist with configuration of 3DS solutions using Google Cloud products. Use of either model does not guarantee compliance to PCI 3DS; however, the impacts described herein and within the Google Cloud Platform: Shared Responsibility Matrix may be useful for considering either such approach. Similarly, these models provide only a few of the innumerable ways in which Google Cloud products may be configured to satisfy the applicable PCI 3DS controls for a customer environment. Customers should consult with their Google Account Manager, the card brands, and/or a PCI 3DS Assessor for details on the specific impacts of these products for their unique implementation and 3DE.

Within each architecture, several of the high-level impacts are discussed to aid in understanding how this architecture may be configured to satisfy controls within PCI 3DS Core Security Standard. More details on the products identified within each sample architecture may be found in Appendix A. Relationships to specific 3DS controls may be examined in further detail within the Google Cloud Platform: Shared Responsibility Summary matrix, available upon request from the Google Compliance team.

Reference Architecture 1

The below diagram demonstrates a sample use case for an entity providing a 3DS solution using Google Cloud products:

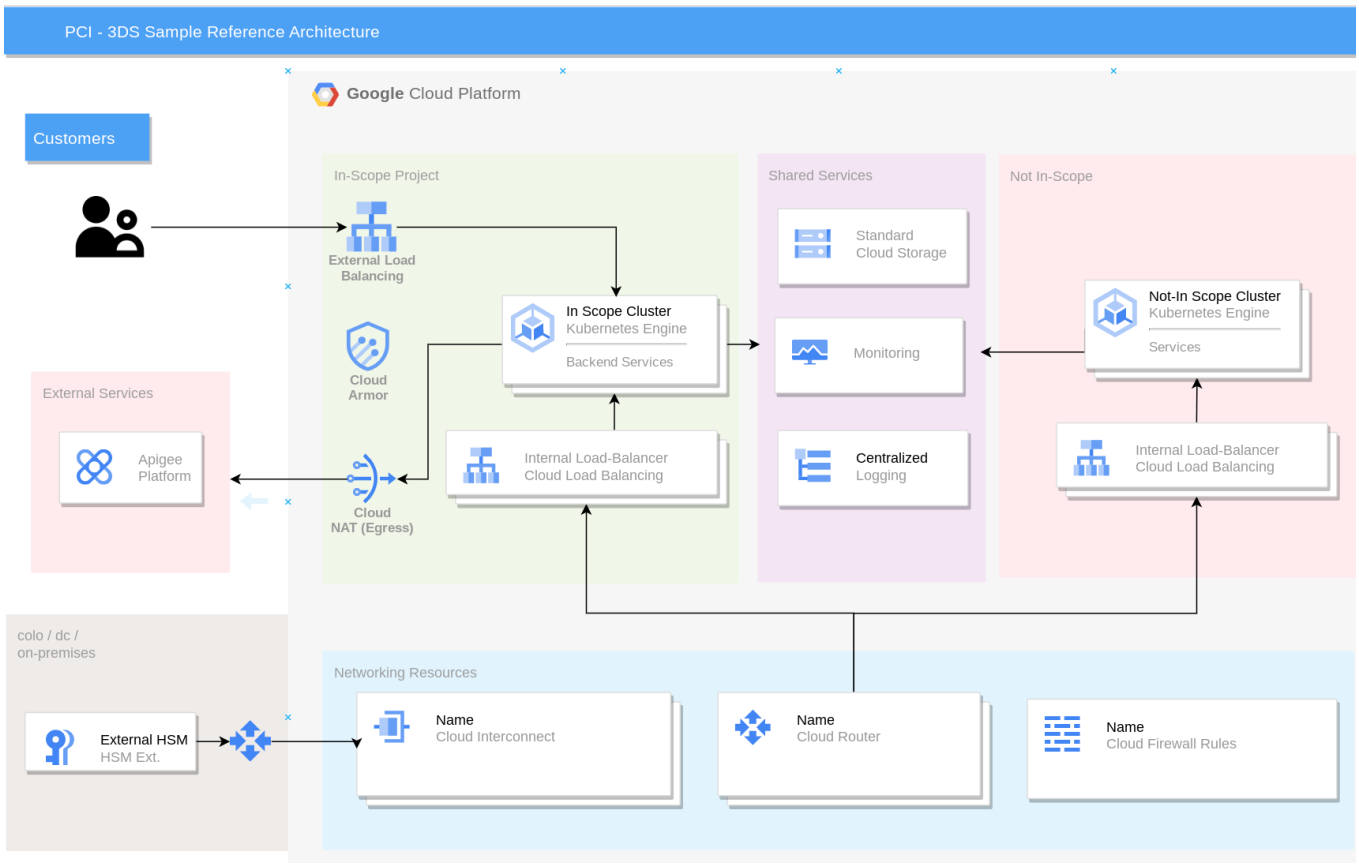

Figure 4: Sample 3DS Reference Architecture indicating 3DE Scope and External HSM

In this example, the customer is hosting a 3DSS.

The 3DSS provides the interface between the consumer's device and the DS. To perform this function, the 3DSS will:

- Receive requests initiated from the 3DS requestor environment (often the merchant environment).
- Collect data elements that compose the ultimate 3DS message (e.g., data entered by the cardholder from a phone or tablet, a merchant, and/or customer data on file within the 3DSS).
- Authenticate the DS.
- Initiate the 3DS authenticated transaction.
- Provide a link between the merchant and their acquirer for authorization requests.

In this example, the following Google Cloud services are used to power the 3DSS 3DE:

- Inbound requests are received from customer devices, protected by Cloud Armor.
- These inbound request TLS 1.2 HTTPS transmissions are load-balanced between GKE clusters.
- All key related activities are directed to Cloud HSM or to an external HSM via Cloud Interconnect (where the customer wishes to leverage existing HSMs within Google Marketplace or entity-hosted environments).
- The outbound 3DS message is then formatted and routed through Cloud NAT to enumerated endpoints, managed by Apigee, to the DS or any other authorized acquirer systems.
- All application activities are logged using Google Monitoring and Google Logging. These controls are configured at the product level, and logs are exported to BigQuery for analysis.
- Remote access from authorized systems is routed to the appropriate cluster, authenticated via IAM, and protected using Google VPN and/or BCE.

Reference Architecture 2

The diagram below demonstrates a second sample use case for a company that has implemented a 3DS DS component within their Google Cloud hosted environment, showing detail for interactions with hypothetical 3DSS and ACS entities, as well as logical flow for remote administration. Furthermore, in this example, the customer may be eligible for use of Hosted Private HSM however, availability of this product is limited and should not be assumed for all customers:

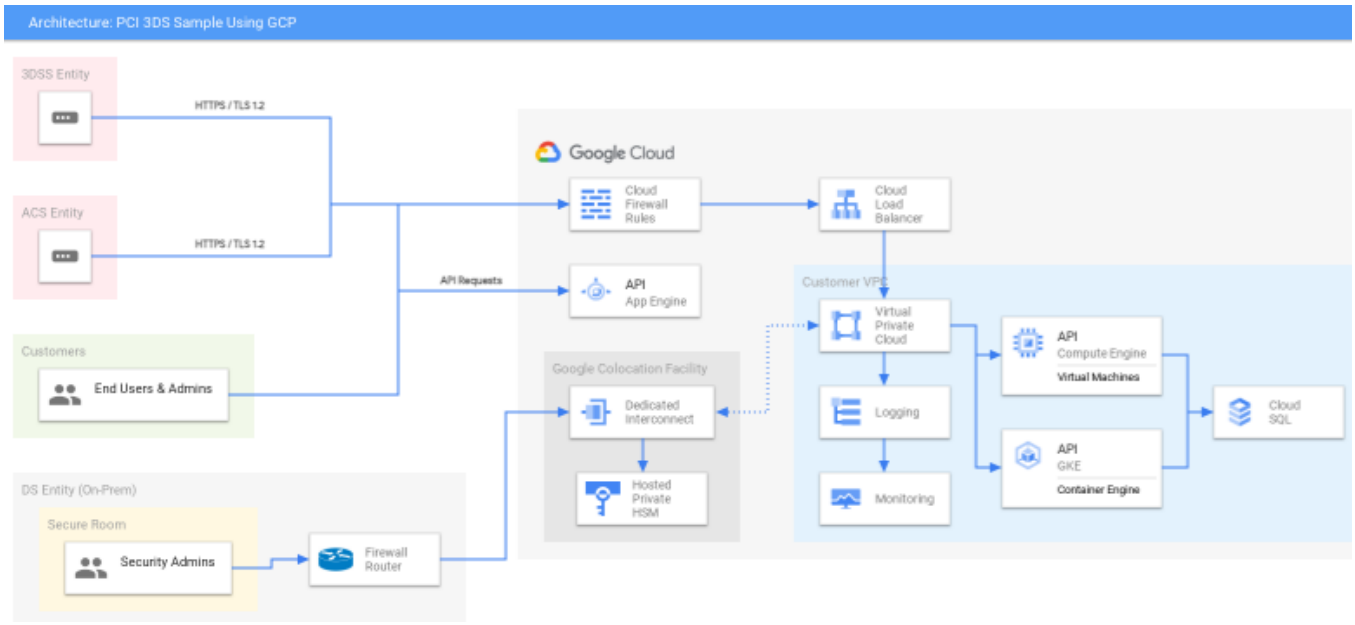

Figure 5: Sample 3DS Reference Architecture with Logical Flow and Hosted Private HSM

For this example, an 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 above.

The DS 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 5 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 the GFE using configured MFA controls.
- The DS entity's 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 HSM, 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 Hosted Private HSM for management of its 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 Balancing.
- Google Cloud's VPC service provides the capability to secure the perimeter and constrain data.

Appendix D - Resources

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

- PCI 3DS Core Security Standard v1.0 Requirements
  https://www.pcisecuritystandards.org/document_library/?category=3DS
- PCI 3DS Data Matrix:
  https://www.pcisecuritystandards.org/documents/PCI-3DS-Data-Matrix-v1_1.pdf
- PCI DSS
  - v4.0 Requirements:
    https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf
  - 3.2.1 Requirements:
    https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v3-2-1-r1.pdf
- EMVCo 3DS Specification
  https://www.emvco.com/wp-content/uploads/documents/EMVCo_3DS_CoreSpec_v2.3.1_20220831.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

Legal Disclaimer

This white paper is provided by Coalfire Systems, Inc., or its subsidiaries ("Coalfire") for informational purposes only. This white paper is the property of Coalfire and is protected by U.S. and international copyright laws. Unauthorized use, reproduction, or distribution of this white paper, in whole or in part, is strictly prohibited. Factual information included in this white paper has been taken from sources that Coalfire believes to be reliable, but its accuracy, completeness, or interpretation cannot be guaranteed. Information is current as of the date of this white paper only and is subject to change without notice. This white paper is provided "as-is" with no warranties, including any warranty of merchantability, fitness for a particular purpose, and non-infringement. Coalfire expressly disclaims all liability arising from or relating to the use of any information or material included in this white paper for any purpose, including any actions taken or not taken based on the contents of this white paper. You are solely responsible for making your own independent assessment of the information in this white paper and for the development, implementation, and execution of your information security program. For questions regarding any legal or compliance matters referenced in this white paper, you should consult your legal counsel, security advisor, or the relevant standard authority.

About the Authors

Bhavna Sondhi, *Senior Manager, Technical Solutions*

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 15 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.

Sam Pfanstiel, Ph.D., *Principal*

Sam Pfanstiel is responsible for providing advisory and assessment services for 3DS solutions and components, as well as identifying security and compliance impacts within the PCI DSS, P2PE, PIN, SSF Secure Software, and Secure SLC programs. Sam has 25 years of experience in a broad spectrum of disciplines, including payment security, card brand compliance, fraud, application security, mobile security, infrastructure, software development, and cryptography.

About Coalfire

The world's leading technology infrastructure providers, SaaS companies, and enterprises – including the top 5 cloud service providers and 8 of the top 10 SaaS businesses – rely on Coalfire to strengthen their security posture and secure their digital transformations. As the largest firm dedicated to cybersecurity, Coalfire delivers a comprehensive suite of advisory and managed services, spanning cyber strategy and risk, cloud security, threat and vulnerability management, application security, privacy, and compliance management. A proven leader in cybersecurity for the past 20 years, Coalfire combines extensive cloud expertise, advanced technology, and innovative approaches that fuel success. For more information, visit **Coalfire.com**.

WP_Google_PCI_3DS_20221005