WHITE PAPER

AWS

PCI 3DS WHITEPAPER

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

COALFIRE

North America | Europe
877.224.8077 | info@coalfire.com | Coalfire.com

TABLE OF CONTENTS

Executive Summary **3**

Introduction to 3DS 3

Relationship Between PCI DSS and 3DS Core Security Standard **5**

Shared Security Responsibilities - AWS and the PCI 3DS Entity **6**

PCI 3DS Part 1: Baseline Security Requirements 6

PCI 3DS Part 2: Security Requirements to Protect 3DS Data and Processes 7

Use Case - Implementation of ACS in an AWS Environment **9**

Conclusion **11**

Resources **12**

EXECUTIVE SUMMARY

Amazon Web Services (AWS) engaged Coalfire Systems, Inc. (Coalfire), an independent Payment Card Industry (PCI) certified qualified security assessor to conduct an assessment of their Payment Card Industry (PCI) 3-D Secure (3DS) environment (3DE). The assessment was conducted from February 2020 to June 2020, and the resulting Attestation of Compliance (AOC) was provided to AWS on October 15, 2020. During the assessment, Coalfire validated the AWS 3DE against the PCI 3DS Core Security Standard and determined the 3DE was compliant for the requirements applicable to AWS, as AWS provides only hosting services to customers. The PCI 3DS AOC can be retrieved from AWS to confirm the 3DS compliance for AWS environment.

The goal of this white paper is to provide AWS customers with guidance on the PCI 3DS Core Security Standard and its applicability to the AWS hosted environment. Entities performing 3DS functions who use the AWS environment for hosting their 3DE are subject to the PCI 3DS Core Security Standard requirements. 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 AWS and its entities to meet the 3DS Core Security Standard requirements. The AWS 3DS Responsibility Matrix can also be retrieved from AWS to understand the shared responsibilities between AWS and 3DS entities using AWS environment for maintaining 3DS compliance.

INTRODUCTION TO 3DS

3DS is a specification aimed at securing authentication and identity verification in mobile and browser-based applications. It is defined within the EMV 3DS Protocol and Core Functions Specification document, which is managed and maintained by EMVCo.

The following three domains are included within 3DS[1]. Figure 1 depicts the interaction between the three domains and its components:

- Merchant or Acquirer Domain – 3-D Secure 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 – 3-D Secure transactions are switched between the Acquirer Domain and 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 – 3-D Secure 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)

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

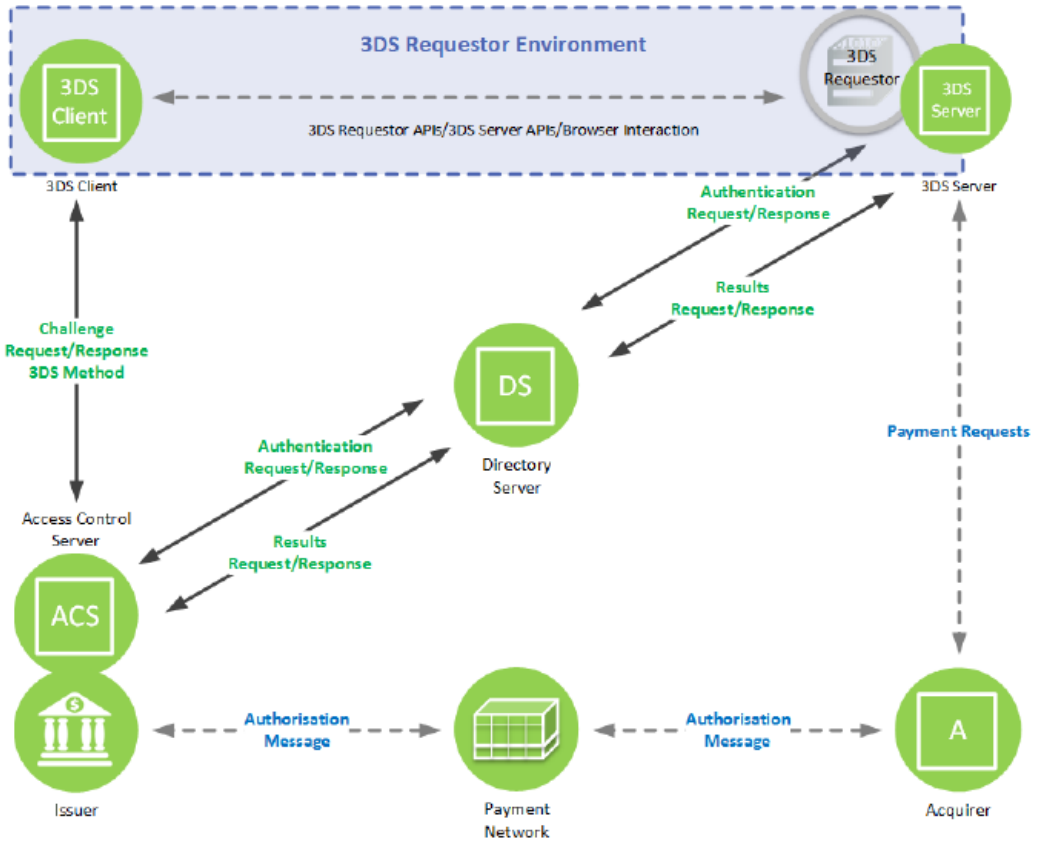

Figure 1: 3-D Secure Domains and Components[2]

The PCI 3DS Core Security Standard applies to environments where 3DS ACS, DS, or 3DS Server (3DSS) functions are performed. A 3DE contains the system components involved in performing or facilitating 3DS transactions. Other components such as network devices, servers, applications, and computing devices are also part of 3DE.

Per 3DS Core Security Standard v1.0, Oct 2017 Page 11 Use of Third-Party Service Providers /Outsourcing[3] Option (a) defined below, AWS is a service provider to 3DS entities:

"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."

As a service provider, AWS offers customers the ability to host their 3DE within AWS environment, thus requiring AWS to share certain responsibilities with 3DS entities that are identified within the AWS 3DS Responsibility Matrix.

[2] https://www.emvco.com/terms-of-use/?u=/wp-content/uploads/documents/EMVCo_3DS_Spec_v220_122018.pdf
[3] https://www.pcisecuritystandards.org/documents/PCI-3DS-Core-Security-Standard-v1.pdf

The 3DS Core Security Standard defines the following functions performed or provided by the EMV® 3DS entities[4]:

- **3DS Access Control Server (ACS)** contains the authentication rules and is managed within the issuer domain.
- **3DS Server (3DSS)** provides the functional interface between the 3DS requester environment and the DS.
- **3DS Directory Server (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 3DS specification guide[5] and PCI 3DS Core Security Standard[6].

RELATIONSHIP BETWEEN PCI DSS AND 3DS CORE SECURITY STANDARD

The PCI DSS and PCI 3DS Core Security Standard are independent standards and are therefore assessed separately. A 3DE can be a part of the PCI cardholder data environment (CDE) or can be completely separate. The payment brand identifies if an entity is required to comply with 3DS Core Security Standard requirements, PCI DSS, or both.

AWS provides networking, computing, and storage services that may be used to support customers' solutions for 3DS functions. AWS does not perform the functions of 3DSS, DS, and ACS directly, but instead manages the 3DS Combined Environment, as shown in Figure 2, and supports the 3DS Standalone Environment for customers where responsibilities are shared between AWS and the customer.

The PCI 3DS Core Security Standard requirements are organized in 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 to protect 3DS data and processes.

[4] https://www.pcisecuritystandards.org/documents/PCI-3DS-Core-Security-Standard-v1.pdf
[5] https://www.emvco.com/terms-of-use/?u=/wp-content/uploads/documents/EMVCo_3DS_Spec_v220_122018.pdf
[6] https://www.pcisecuritystandards.org/documents/PCI-3DS-Core-Security-Standard-v1.pdf

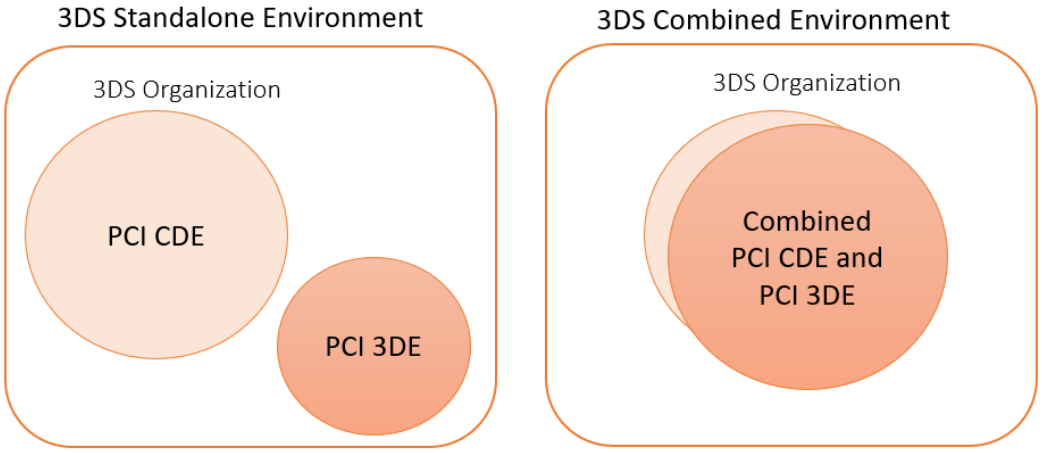

Figure 2: 3DE Scenarios

SHARED SECURITY RESPONSIBILITIES - AWS AND THE PCI 3DS ENTITY

AWS provides coverage for the 3DS controls applicable to AWS as a hosting service provider and is in compliance with PCI 3DS as identified in the AWS 3DS AOC which can be retrieved from AWS; however, 3DS customers utilizing the AWS environment are responsible for most 3DS controls and their own 3DS compliance. Some 3DS requirements may be satisfied by the customer's use of AWS services, but most requirements are either shared responsibilities between the AWS customer and AWS, or entirely the customer's responsibility. The following sections describe the responsibilities that AWS assumes for the services offered and the customer's responsibilities when utilizing the in-scope AWS services.

AWS provides hosting services to its customers. Customers using AWS are responsible for their own PCI 3DS compliance; specifically, all logical security controls to protect 3DS functions are the responsibility of AWS customers. AWS is responsible for protecting the infrastructure, composed of the hardware, software, networking, and facilities, that runs the AWS cloud services.

PCI 3DS PART 1: BASELINE SECURITY REQUIREMENTS

The AWS 3DE is part of the AWS CDE. AWS PCI DSS compliance satisfies the AWS PCI 3DS Core Security Standard Part 1 requirements.

The PCI 3DS Core Security Standard Part 1 requirements, the PCI DSS corresponding requirements, and the responsibilities of AWS and AWS customers are outlined below:

3DS PART 1 BASELINE REQUIREMENT		CORRESPONDING PCI DSS REQUIREMENT	RESPONSIBILITY SUMMARY
P1-1	Maintain security policies for all personnel	• Requirement 12	The AWS PCI DSS service provider environment is compliant with PCI DSS controls and is utilized to meet 3DS Part 1 controls. The AWS PCI DSS responsibility matrix outlines the services covered under PCI DSS validation and the responsibilities
P1-2	Secure network connectivity	• Requirement 1 • Requirement 10 • Requirement 11	

3DS PART 1 BASELINE REQUIREMENT		CORRESPONDING PCI DSS REQUIREMENT	RESPONSIBILITY SUMMARY
P1-3	Develop and maintain secure systems	• Requirement 2 • Requirement 6	of AWS and AWS customers to maintain a compliant PCI DSS environment If AWS services are utilized for 3DS, AWS customers should: • Retrieve the current PCI DSS and 3DS AOC from AWS. • Retrieve the PCI DSS Responsibility Matrix. • Maintain written agreements with AWS to ensure the security responsibilities are understood and acknowledged. • Manage and implement controls as outlined in the PCI DSS Responsibility Matrix. • Periodically verify that agreed upon responsibilities are met. • Confirm the in-scope services and specific actions to be implemented to meet the controls identified within PCI DSS and 3DS Core Security Standard.
P1-4	Vulnerability management	• Requirement 5 • Requirement 6 • Requirement 11	
P1-5	Manage access	• Requirement 7 • Requirement 8	
P1-6	Physical security	• Requirement 9	
P1-7	Incident response preparedness	• Requirement 10 • Requirement 12	

Table 1: PCI 3DS Core Security Standard Part 1 Requirements

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

AWS meets the necessary 3DS requirements in Part 2, however customers are responsible for meeting the responsibilities partially when AWS environment is utilized. The following documents are required if AWS services are used by the customer to understand the shared responsibilities and the in-scope services validated for 3DS and PCI DSS compliance:

- AWS PCI 3DS and PCI DSS Responsibility Matrix: These documents outline the in-scope services that can be used to meet Part 2 of the 3DS Core Security Standard requirements. There are various responsibilities shared between AWS and AWS customers, and the services utilized are required to be configured as per AWS guidelines to meet the necessary controls for the 3DE. These responsibility matrix documents can be retrieved from AWS.
- AWS PCI 3DS and PCI DSS AOC: The current attestation documents for validated compliance frameworks can be retrieved from AWS.

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

3DS PART 2 REQUIREMENTS			RESPONSIBILITY SUMMARY
P2-1	Validate scope	1.1 Scoping	The AWS managed environment consists of underlying physical and logical infrastructure that supports the AWS services, including servers, operating systems, hypervisor, and control environment for management and operation of the AWS services.

3DS PART 2 REQUIREMENTS			RESPONSIBILITY SUMMARY
P2-2	Security governance	2.1 Security governance 2.2 Manage risk 2.3 Business as usual (BAU) 2.4 Manage third-party relationships	AWS customers will need to 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	Requirements 1, 2, and 6 of the PCI DSS outline the in-scope services for protection of systems and applications. AWS customers will need to implement these services as per AWS guidelines to meet the PCI 3DS controls. The management of availability zones is not directly covered under PCI DSS requirements, but will need to be managed by the customers for their PCI 3DS environment.
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	Requirements 1, 2, 7, and 8 of the PCI DSS outline the in-scope services for securing logical access. AWS customers will need to implement these services as per AWS guidelines to meet the PCI 3DS controls.
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	Requirements 2,3, 4, and 10 of the PCI DSS outline the in-scope services for data transmission, Transport Layer Security (TLS) configurations, data storage, and monitoring of transactions that the AWS customer will need to implement as per AWS guidelines to meet the PCI 3DS controls.
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)*	If AWS offered CloudHSM option is utilized, AWS customer will need to implement the CloudHSM service as per AWS guidelines to meet the PCI 3DS controls.
P2-7	Physically secure 3DS systems	7.1 Data center security 7.2 CCTV	AWS maintains the physical and media handling controls for the AWS PCI DSS environment where 3DS systems are hosted and meets the necessary 3DS requirements for their customers as noted within the PCI 3DS AOC.

Table 2: PCI 3DS Part 2 Requirements

USE CASE - IMPLEMENTATION OF ACS IN AN AWS ENVIRONMENT

This section describes a hypothetical use case for a generic company ("Company XYZ") that has implemented 3DS ACS within their AWS environment. Company XYZ is an online issuer processor performing 3DS functions in support of card brands issued. They are required to allow an incoming authorization request, which requires the additional authentication specified in the EMVCo 3DS protocol.

It is assumed that the brand payment brand identified 3DS protocol is implemented by Company XYZ for the purposes of this use case. The application is deployed within Company XYZ's own virtual private cloud in AWS and integrated within the existing PCI DSS environment, as depicted in the architecture diagram below.

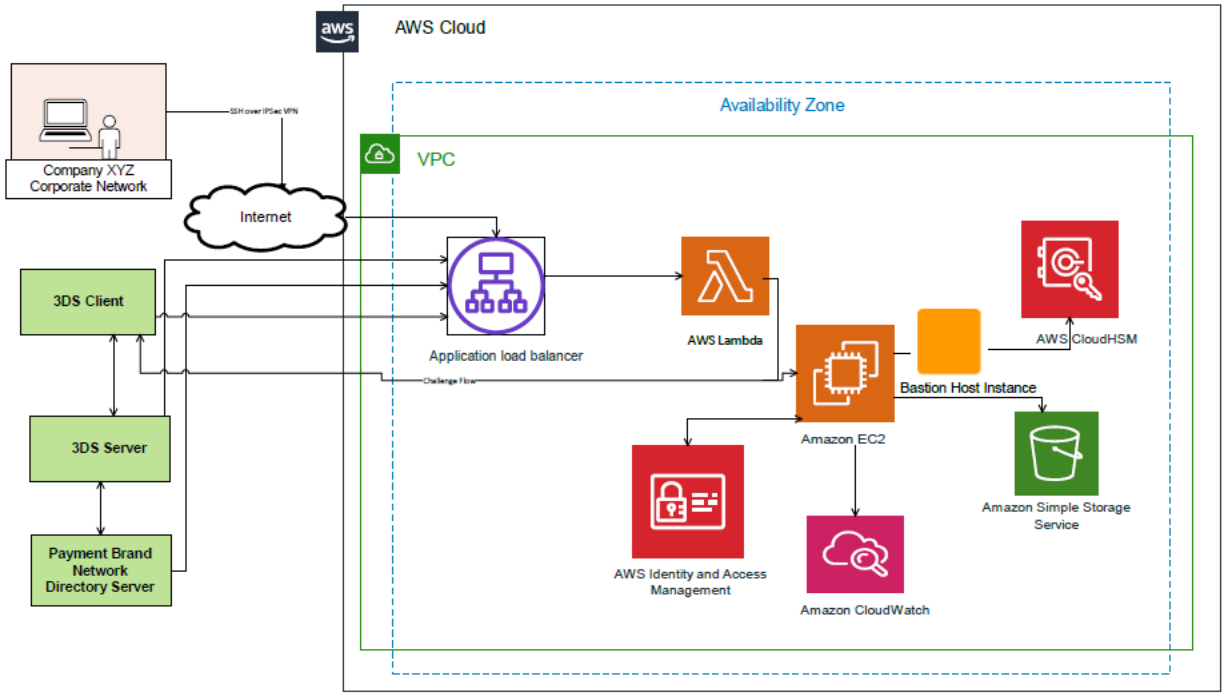

Figure 3: Company XYZ AWS 3DS Architecture Diagram

The following AWS services are utilized by Company XYZ for this hypothetical implementation of the 3DS ACS:

- AWS Lambda: The 3DS application entry point is architected as a microservice leveraging AWS Lambda for the challenge HTML page rendering.
- AWS Application Load Balancers: Used for balancing load to the hypothetical 3DS application service.
- Amazon Virtual Private Cloud (VPC): Provides logical isolation (networking, computer and memory) of the AWS Cloud.
- AWS CloudHSM: Used for managing sensitive authentication operations, cryptographic processes, and key management.

- Amazon Elastic Compute Cloud (EC2): Web server instance used for reverse proxying the connections to the 3DS environment.
- Amazon EC2 Web Server: Tomcat web application server instance for hosting 3DS applications. The web application server is configured as per guidelines to meet server hardening requirements as AWS does not manage their customers' EC2 configurations.
- AWS Classic Load Balancer Service: Used for incorporating load balancing across EC2 instances and applications built on Amazon EC2.
- Amazon Simple Storage Service (S3): Used for storage of data that are integrated with the EC2 server instances. Amazon S3-provided default encryption for the bucket is utilized for the protection of data during storage. In this hypothetical scenario, the default option used server-side encryption with customer master keys (CMKs) stored in the AWS Key Management Service (KMS).
- AWS Identity and Access Management (IAM): Used for configuring access across AWS services and resources.
- AWS Config: Used for assisting with inventory management and configuration changes for enabling security and governance.
- AWS State Manager: Used for configuring and managing the state of 3DS applications.
- AWS CloudWatch: Used for debug logging for the AWS Lambda microservice.
- AWS CloudTrail: Used for event monitoring for the whole VPC.
- AWS Web Application Firewall (WAF): Used for the protection of Company XYZ-developed web applications or application programming interfaces (APIs) against the common client-side attacks.
- Amazon API Gateway: Used for creating, publishing, maintaining, monitoring, and securing APIs.

To comply with the requirements within Part 2 of the PCI 3DS Core Security Standard, listed below, Company XYZ configured the above services according to the guidelines from AWS:

Requirement P2-1: Scoping

If integrated with the AWS PCI DSS CDE environment, the 3DS solution is generally well contained due to the application residing in its own virtual private cloud in AWS. Any systems connected to the 3DE or systems that are not part of AWS are scoped and managed separately by Company XYZ.

Requirement P2-2: Security governance

Various 3DS responsibilities were combined into PCI DSS responsibilities. The security objectives, roles and responsibilities, implementation of risk management strategy; and management of third-party relationships controls were defined for 3DE being a subset of the PCI DSS CDE.

Requirement P2-3: Protect 3DS systems and applications

Company XYZ could whitelist or permit connections from card networks' API. AWS Security Group configurations blocked all access excluding the access required for payment brands. IAM roles were configured to provide access to resources on a need-to-know basis.

AWS application and network load balancers were leveraged to offer resilience against workloads providing services to the 3DS application developed by Company XYZ. Amazon EC2 with AWS scaling features enabled allows for significant capacity in the 3DS application and essentially add additional resources (compute and memory) as needed. The microservice element of the 3DS application is written directly for the AWS Lambda serverless compute and comes with autoscaling capabilities that enable high availability

and geodiversity. AWS WAF allowed and blocked requests specific to the application and APIs, while the rules and rules group configuration allowed for inspection of web traffic. Amazon CloudWatch was used to monitor the logs from AWS Lambda and application event logs.

Requirement P2-4: Secure logical access to 3DS systems

For the remote protection of AWS resources, Company XYZ used AWS Client VPN with multi-factor authentication configured through Active Directory using certificate-based authentication.

AWS CloudTrail captured all API calls for IAM, while Amazon CloudWatch monitored various AWS resources and the applications residing in the 3DE.

Requirement P2-5: Protect 3DS data

Company XYZ identified the various 3DS sensitive data being stored (temporarily in memory) and transmitted. The protection of 3DS data was enforced using Amazon S3 buckets for restricting application access, AWS CloudHSM for creating and managing key materials, and AWS CloudTrail for bucket logging and monitoring.

Tomcat web servers were configured for appropriate TLS 1.2 or higher protocol with strong cipher suites on the EC2 instance. The AWS API Gateway service was used to create HTTP APIs and integrate with the AWS Lambda function on the backend. API Gateway sends and receives requests and responses. AWS API Gateway was configured to use the TLS 1.2 security policy.

Requirement P2-6: Cryptography and key management

Company XYZ utilized AWS CloudHSM for the management of cryptographic keys (symmetric keys, in this scenario) for the protection of 3DS sensitive data and used the CloudHSM guide for managing the below tasks.

- Generation, storage, import, and export of the symmetric cryptographic keys
- Use of the AES-CBC algorithm and AES-256-bit keys identified within the CloudHSM
- Use of the FIPS-approved random number generator during generation of keys
- Use of CloudTrail for recording user actions on the CloudHSM. The use of bastion is required for ad hoc access to the CloudHSM cluster.

Requirement P2-7: Physically secure 3DS systems

Company XYZ fully relies on AWS PCI DSS and 3DS compliance for this requirement.

CONCLUSION

AWS maintains and manages its own compliance as part of their service provider responsibilities for the PCI 3DS Core Security Standard. 3DS entities that utilize AWS services will need to understand their responsibilities and the in-scope services that will have to be maintained and configured as per the guidance from AWS in order to be compliant for their 3DS environment. 3DS entities will also have responsibilities to meet the PCI 3DS Core Security Standard requirements that are not met by use of AWS services directly.

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

RESOURCES

The following sources provided additional information as guidance for this document.

- PCI 3DS Requirements
- PCI DSS 3.2.1 Requirements
- AWS Compliance: PCI DSS
- AWS Services Security Documentation
- AWS Web Services: Overview of Security Processes

ABOUT THE AUTHOR

Bhavna Sondhi | Principal Consultant

Bhavna Sondhi is the practice subject matter expert for the Solution Validation team at Coalfire. Bhavna performs advisory work and assessments for various payment card industry 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 the teams recognize the importance of secure code development and information security within their operational practices.

ABOUT THE REVIEWER

Andrew Barratt | Managing Principal

Andrew is the head of the Solutions and Investigations practice at Coalfire, carrying almost all the PCI qualifications he is a QSA, PA-QSA, P2PE-QSA, 3DS assessor and a CORE PFI. Andrew is a trusted advisor to large organizations around the world and a regular spokesperson in the media on cyber security issues.

Published October 2020.

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.

Copyright © 2014-2020 Coalfire Systems, Inc. All Rights Reserved. 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.