WHITE PAPER

MICROSOFT AZURE CLOUD PLATFORM

FOR PCI 3DS

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

COALFIRE

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

TABLE OF CONTENTS

Executive Summary **3**
What is 3DS? 3
Relationship Between PCI DSS and 3DS Core Security Standard **5**
Azure 3DS Services **6**
3DS Shared Responsibility Summary **8**
PCI 3DS Part 1: Baseline Security Requirements 8
PCI 3DS Part 2: Security Requirements to Protect 3DS Data and Processes 8
Sample Implementation of ACS Component in an Azure Environment **13**
Requirement P2-1: Scoping 14
Requirement P2-2: Security Governance 14
Requirement P2-3: Protect 3DS Systems and Applications 14
Requirement P2-4: Secure Logical Access to 3DS Systems 15
Requirement P2-5: Protect 3DS Data 15
Requirement P2-6: Cryptography and Key Management 15
Requirement P2-7: Physically Secure 3DS Systems 16
Conclusion **16**
Resources **17**

EXECUTIVE SUMMARY

Microsoft Corporation (“Microsoft”) engaged Coalfire Systems, Inc. (“Coalfire”), a respected Payment Card Industry (PCI) Qualified Security Assessor (QSA) and PCI Three-Domain Secure (PCI 3DS) assessor company to conduct an assessment of their PCI 3-D Secure Environment (3DE), hosted on the Azure cloud platform.

Coalfire conducted assessment activities including document reviews, staff interviews, and data center walkthroughs to validate the Azure 3DE against PCI 3DS Core Security Standard 1.0 from October 2020 to January 2021. An Attestation of Compliance (AOC) document for the PCI 3DS environment assessed was provided to Azure compliance team on 29 January 2021. Coalfire determined that Azure PCI 3DS service provider environment meets the applicable PCI 3DS controls.

Azure provides platform and infrastructure services for customers to host their own 3DE; however, Azure does not develop or provide 3DS component hosted services to end users.

The goal of this white paper is to provide guidance to Azure PCI 3DS customers on the PCI 3DS Core Security Standard and how the Azure 3DE can be utilized to implement a 3DE on the Azure cloud platform. Per PCI SSC FAQ Article 1487[1], a 3DS entity can choose to outsource the hosting and management of its hardware security module (HSM) infrastructure to a third-party service provider if the applicable requirements are met. Entities performing 3DS functions who use the Azure environment for hosting their 3DE are still subject to the PCI 3DS Core Security Standard and must have their environment assessed for all applicable 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 Azure and its entities to meet the 3DS Core Security Standard requirements. Microsoft provides a PCI 3DS responsibility matrix and PCI 3DS AOC for Azure through the Azure compliance team that customers can request to understand the responsibilities between Azure and the 3DS entity and confirm Azure’s compliance for PCI 3DS applicable requirements.

WHAT IS 3DS?

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

The following three domains are included within 3DS[2]:

- **Merchant or Acquirer Domain** – 3DS transactions are initiated from the acquirer domain. The components under this domain are the 3DS requester environment, the 3DS integrator, and the acquirer.

[1] https://pcissc.secure.force.com/faq/articles/Frequently_Asked_Question/Is-an-EMVCo-Letter-of-Approval-required-prior-to-conducting-a-PCI-3DS-Assessment?q=3DS&l=en_US&fs=Search&

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

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

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

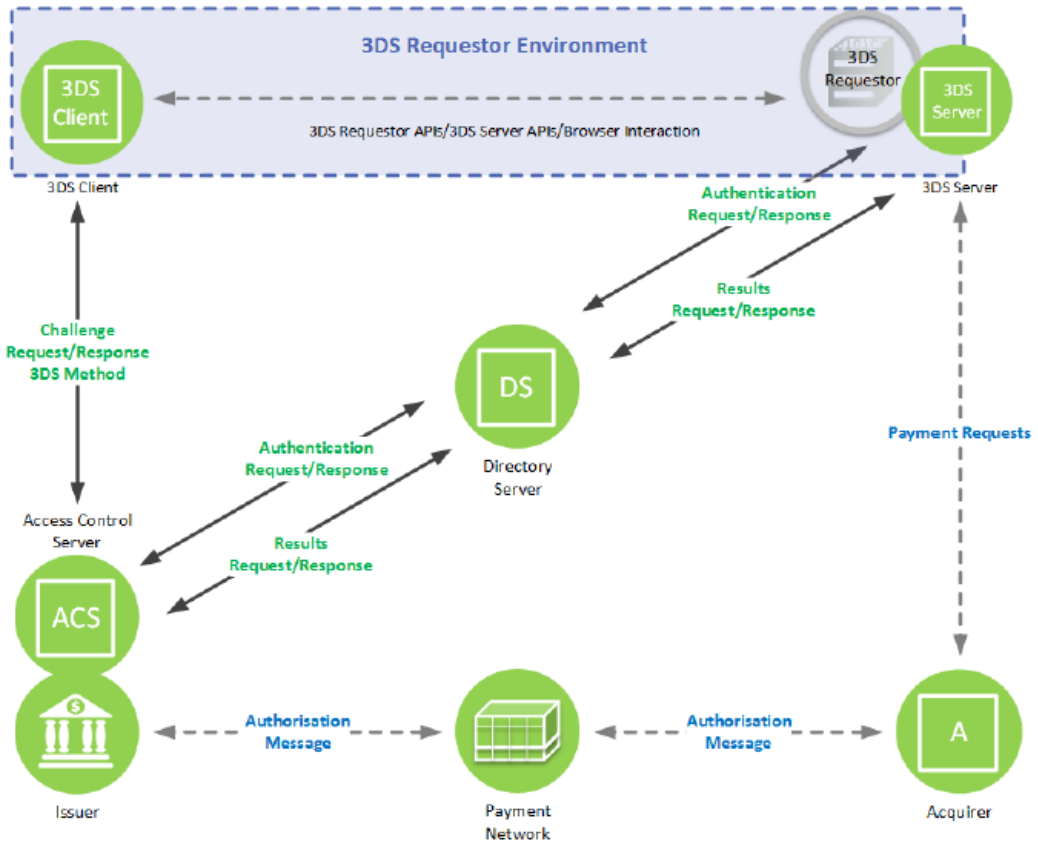

Figure 1: 3-D Secure Domains and Components[3]

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 PCI 3DS Core Security Standard 1.0 page 11, Use of Third-Party Service Providers/Outsourcing[4] Option (a), Azure acts a service provider to 3DS entities that offers HSM hosting and data center environments where infrastructure and services can be hosted:

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

"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."

Azure services can be utilized by 3DS customers to host their 3DE and meet certain applicable controls related to physical security within data center environments. There are various controls that are shared, and 3DS entities are required to ensure that they configure and utilize the services in a manner that meets all applicable PCI 3DS requirements.

The PCI 3DS Core Security Standard defines the following functions performed or provided by the EMV 3DS entities[5]:

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

For more information on the functions performed by the ACS, DS, and 3DSS, please refer to the 3DS specification guide[6] and PCI 3DS Core Security Standard[7].

RELATIONSHIP BETWEEN PCI DSS AND 3DS CORE SECURITY STANDARD

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

The Azure cloud platform offers specific services, outlined in the Azure 3DS Services referenced below, that may be used to support customers' solutions for 3DS functions. The Azure cloud platform does not perform the functions of 3DSS, DS, and ACS directly, but instead manages the 3DS Combined Environment as shown in Figure 2 below. Azure supports the 3DS Standalone Environment for customers where responsibilities are shared between Azure and the customer.

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

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

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

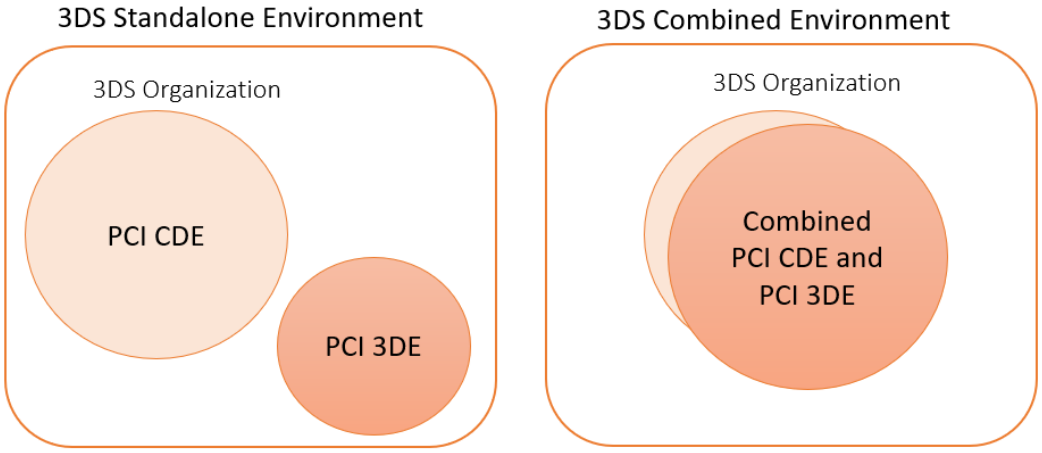

Figure 2: 3DE Scenarios

AZURE 3DS SERVICES

The following offerings are provided by Azure to customers to support their PCI 3DS environments:

AZURE 3DS OFFERINGS/ SERVICES	DESCRIPTION	DOCUMENTATION
Azure Active Directory (AD)	Provides single sign-on (SSO) and multi-factor authentication (MFA).	https://docs.microsoft.com/en-us/azure/active-directory/
Azure Bastion	Provides secure Remote Desktop Protocol (RDP) and Secure Shell (SSH) access to the virtual machines directly through Azure portal.	https://docs.microsoft.com/en-us/azure/bastion/bastion-overview
Azure Cosmos Database (DB)	A fully managed NoSQL database service for modern application development.	https://azure.microsoft.com/en-us/services/cosmos-db/ https://azure.microsoft.com/en-us/blog/a-technical-overview-of-azure-cosmos-db/
Azure Database for MySQL	Focuses on application development.	https://docs.microsoft.com/en-us/azure/mysql/
Azure Dedicated HSM	A Federal Information Processing Standard (FIPS) 140-2 Level 3 certified HSM. All cryptographic processes can be managed by end users through the Azure portal.	https://docs.microsoft.com/en-us/azure/dedicated-hsm/
Azure Domain Name System (DNS)	Can be used to host DNS in Azure alongside the applications.	https://docs.microsoft.com/en-us/azure/dns/dns-overview
Azure Kubernetes Service	Provides options for the deployment and management of containerized applications.	https://docs.microsoft.com/en-us/azure/aks/intro-kubernetes
Azure Load Balancer	Provides high availability and network performance to applications.	https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-overview

AZURE 3DS OFFERINGS/ SERVICES	DESCRIPTION	DOCUMENTATION
Azure Monitor	Collects and analyzes data from Azure and on-premises environments.	https://docs.microsoft.com/en-us/azure/azure-monitor/overview
Azure Policy	An option to support resource governance by creating policies in Azure.	https://docs.microsoft.com/en-us/azure/governance/policy/overview
Container Registry	Provides capabilities to build, store, secure, scan, replicate, and manage container images and artifacts.	https://docs.microsoft.com/en-us/azure/container-registry/
Event Hubs	A big data streaming platform and event ingestion service. The service can be used for managing events for various scenarios, such as anomaly detection, application logging, transaction processing, and live dashboarding.	https://docs.microsoft.com/en-us/azure/event-hubs/event-hubs-about
ExpressRoute	Can be used to create private connections between Azure data centers and infrastructure on customer premises or in a colocation environment.	https://docs.microsoft.com/en-us/azure/expressroute/
Key Vault	This service can be used to securely store cryptographic keys and other secrets used by cloud applications and services. *This product is available for non-3DS-ACS and DS environments only.*	https://docs.microsoft.com/en-us/azure/key-vault/
Redis Cache	Provides an in-memory data store based on Redis software. Azure Cache for Redis can be used as a distributed data or content cache, a session store, a message broker, or similar.	https://docs.microsoft.com/en-us/azure/azure-cache-for-redis/cache-overview
Security Center	Used for security posture management and threat protection for hybrid cloud workloads.	https://docs.microsoft.com/en-us/azure/security-center/security-center-introduction
Storage	A cloud storage solution is offered to help meet data storage and performance needs for applications.	https://docs.microsoft.com/en-us/azure/storage/
Virtual Machine Scale Sets	Can be used for creating and managing a group of load-balanced virtual machines (VMs) for deployment and management.	https://docs.microsoft.com/en-us/azure/virtual-machine-scale-sets/
VMs	Provides on-demand, scalable computing resources intended to provide more control over the computing environment without having to buy and maintain physical hardware.	https://docs.microsoft.com/en-us/azure/virtual-machines/windows/overview
Virtual Network (VNet)	Provides an isolated environment to run virtual machines and applications. It enables the Azure resources to securely communicate with each other over the Internet or on premises.	https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview
Virtual Wide Area Network (WAN)	Provides a networking service. Functionalities such as networking, security, and routing can be configured under a single operational interface.	https://docs.microsoft.com/en-us/azure/virtual-wan/

Table 1: Azure cloud platform offerings

3DS SHARED RESPONSIBILITY SUMMARY

Azure 3DS customers are responsible for ensuring that they meet all 3DS controls for 3DS compliance by configuring and managing the services hosted in the Azure cloud platform. The responsibility for each 3DS requirement can be verified via the PCI 3DS Responsibility Matrix available from the Azure compliance team upon request. Below is a high-level selection partial responsibilities that Azure shares with its customers:

- The Azure cloud platform provides services and offerings identified in the PCI 3DS AOC. All logical security controls to protect 3DS functions are responsibility of the customer.
- The Azure cloud platform provides PCI-DSS and PCI-3DS-compliant hosting and service platform data center environments in which Azure manages the physical security controls within Azure data centers.
- The Azure cloud platform provides a FIPS 140-2 Level 3 certified Azure Dedicated HSM offering; however, the key management and remote management of HSMs is the customer's responsibility.

  For ACS and DS environments, a logical, non-console access solution is not offered by Azure. It is the customer's responsibility to ensure that the non-console access solution is evaluated by an independent laboratory.
- The Azure cloud platform protects infrastructure, including hardware and software; however, customers are required to implement and configure the service offerings by Azure per 3DS requirements.

The following subsections describe the responsibilities that Azure assumes for the services offered and the customer's responsibilities when utilizing the in-scope Azure services.

PCI 3DS PART 1: BASELINE SECURITY REQUIREMENTS

Azure leverages PCI DSS compliance to meet PCI 3DS Core Security Standard Part 1 requirements, as Azure 3DE is part the Azure PCI DSS CDE. Azure customers are, however, responsible for complying with all 3DS Part 1 requirements. If Azure services are utilized, there may be certain responsibilities shared with Azure, and customers should be aware of the below information to maintain their compliance for 3DS:

- **Azure PCI DSS and PCI 3DS AOC** – The AOC documents for Azure should be retrieved from the Azure Compliance team to confirm Azure's compliance for the services offered.
- **Azure PCI DSS and PCI 3DS Responsibility Matrix** – The shared responsibility matrix identifies the responsibilities between Azure and its customers.
- **Contracts and Agreements** – Written contracts and agreements with Azure are required to ensure that security responsibilities are understood and acknowledged between each entity. These documents should be reviewed at least annually to ensure that agreed-upon requirements are met.
- **Implementation of Services** – Azure customers should identify the in-scope services and ensure that they are implemented and configured in accordance with Azure guidelines as well as in compliance with PCI requirements.

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

Azure 3DS environment meets the applicable requirements identified within PCI 3DS Part 2 as demonstrated in PCI 3DS AOC, but there are responsibilities that are partially shared with the customer for

the services it offers. It is important for customers to retrieve the below documents to understand the services offered for PCI 3DS and customer responsibilities for meeting controls:

- **Azure PCI 3DS Responsibility Matrix** – This document outlines 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 Azure and Azure customers, and the services utilized are required to be configured as per Azure guidelines to meet the necessary controls for the 3DE. The responsibility matrix documents can be retrieved from Azure.
- **Azure PCI 3DS AOC** – The current PCI 3DS attestation document for validated compliance frameworks can be retrieved from Azure.

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

3DS PART 2 REQUIREMENTS			RESPONSIBILITY SUMMARY
P2-1	Validate scope	1.1 Scoping	**Azure:** Azure provides a platform for 3DS implementation by the customer and does not directly store, process, or transmit 3DS data. Azure has identified 3DS in-scope services; these are hosted within the 3DE. The Azure environment includes infrastructure, development, operations, management, support and the in-scope services. **Customers:** Azure 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	**Azure:** Azure meets the applicable controls for their 3DE as identified within the PCI 3DS AOC. **Customers:** Azure 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	**Azure:** Azure meets the applicable controls for their 3DE as identified within the PCI 3DS AOC. Some controls are specific to managing traffic between 3DS components, and Azure does not directly handle those services. **Customers:** Azure customers are responsible for implementing the in-scope services per Azure guidelines to meet the PCI 3DS controls. See the Azure 3DS Services section and the security baseline documentation at the following link for additional details: https://docs.microsoft.com/en-us/azure/cloud-services/security-baseline. For maintaining the availability of 3DS operations, refer to the following link: https://docs.microsoft.com/en-us/azure/availability-zones/az-region.

3DS PART 2 REQUIREMENTS			RESPONSIBILITY SUMMARY
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	**Azure:** Azure meets the applicable controls for their 3DE as identified within the PCI 3DS AOC. **Customers:** Customers are responsible for configuring the services and logical access for the in-scope services for their 3DE. See the Azure 3DS Services section and the security baseline documentation at the following link for additional details: https://docs.microsoft.com/en-us/azure/cloud-services/security-baseline. Additional resources for configurations are identified below: • See the Network Security section that identifies the Azure network security group access rules to be configured at the following link: https://docs.microsoft.com/en-us/azure/security/benchmarks/security-control-network-security. • See the Identity and Access Control section that identifies the Azure AD MFA functionality for the Azure environment at the following link: https://docs.microsoft.com/en-us/azure/security/benchmarks/security-control-identity-access-control. • Service offerings such as Virtual Network , Azure Load Balancer, Azure DNS, Azure Security Center, Azure Policy, Azure Monitor, and Azure Kubernetes Service require configurations by the customer to be able to function in a compliant manner.
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	**Azure:** Azure meets the applicable controls for their 3DE as identified within the PCI 3DS AOC. **Customers:** Customers are responsible for configuring the services and protecting the 3DS data within their 3DE. See the Azure 3DS Services section and the security baseline documentation at the following link for additional details: https://docs.microsoft.com/en-us/azure/cloud-services/security-baseline. For the application services offered by Azure, the following configurations are required to be performed by customers: • Transmission – Enforce HTTPS option: – https://docs.microsoft.com/en-us/azure/app-service/configure-ssl-bindings#enforce-https • TLS Configurations: – https://docs.microsoft.com/en-us/azure/app-service/configure-ssl-bindings#enforce-tls-versions – https://docs.microsoft.com/en-us/azure/cloud-services/cloud-services-configure-ssl-certificate-portal – To modify the list of ciphers, customers can refer to the following links:

3DS PART 2 REQUIREMENTS			RESPONSIBILITY SUMMARY
			▪ https://docs.microsoft.com/en-us/azure/app-service/environment/app-service-app-service-environment-custom-settings ▪ https://docs.microsoft.com/en-us/windows/win32/secauthn/cipher-suites-in-schannel?redirectedfrom=MSDN • Storage of data – Azure offers Azure Cosmos DB, Azure Database for MySQL, and core storage services options for storing data. The key management processes, however, are required to be performed on the HSM. See the following link for additional details: – https://docs.microsoft.com/en-us/azure/storage/common/storage-introduction?toc=/azure/storage/blobs/toc.json • Monitoring and alerting – Customers must monitor 3DS transactions but can utilize services such as Azure Security Center for capturing the information. See the following link for additional details: – https://docs.microsoft.com/en-us/azure/security-center/tutorial-security-policy – Azure Monitor can be used to identify issues affecting the applications and resources and be used for investigation purposes. See the following link for additional details: ▪ https://docs.microsoft.com/en-us/windows-server/storage/storage-spaces/configure-azure-monitor
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)	**Azure:** Azure offers services such as Azure Key Vault and Azure Dedicated HSM for key management. Microsoft is partially responsible for meeting controls applicable to their 3DE. • Azure Key Vault Service – Azure partially manages HSM and cryptographic keys and meets the applicable controls for their 3DE as identified in the PCI 3DS AOC. See the following link for additional details: – https://docs.microsoft.com/en-us/azure/key-vault/general/basic-concepts – *Note that Azure Key Vault is not recommended for use in ACS and DS 3-D Secure environment as it does utilize FIPS 140-2 Level 3 certified HSM.* • Azure Dedicated HSM Service – Azure offers a FIPS 140-2 Level 3 certified HSM that uses the Thales Luna K7 Cryptographic Module (https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/3205) single-tenant device option for administrative and full control of the HSM appliance. Azure only provides instructions for the initial provisioning or deployment within the environment. Azure does not manage any cryptographic key processes for the Azure Dedicated HSM. See the following link for additional details:

3DS PART 2 REQUIREMENTS			RESPONSIBILITY SUMMARY
			– https://docs.microsoft.com/en-us/azure/dedicated-hsm/tutorial-deploy-hsm-cli – https://docs.microsoft.com/en-us/azure/dedicated-hsm/tutorial-deploy-hsm-powershell **Customers:** Azure customers are responsible for managing all cryptographic key management processes for their own 3DE when utilizing any HSM service. It is the customer's responsibility to ensure that the HSMs used within the 3DS environment for managing ACS and DS components are certified at FIPS 140-2 Level 3 (overall) or higher. Azure customers are also responsible for securing physical access to the area or room where non-console access to the HSM is initiated from. • Azure Key Vault Service – Azure customers are responsible for securing the key vault, managing the keys as identified in the guidelines . Please refer to the following link for additional details: https://docs.microsoft.com/en-us/azure/key-vault/general/developers-guide. • Azure Dedicated HSM Service – If Azure Dedicated HSM service is utilized, customers are responsible for handling the cryptographic key management processes, including the provisioning of HSM and securing logical access to HSMs for ACS and DS 3DS environment as identified within the 3DS requirement. The FIPS HSM security policy, Thales HSM documentation should be utilized for configuring the HSM to meet all the controls. See the following link for additional details: – https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp3205.pdf – It is the customer's responsibility to utilize non-console access to the HSM that complies with the current version of International Organization for Standardization (ISO) 13491. Please refer to following links for an understanding of the client software's and the PIN Entry Device's (PED's) uses for authentication to the HSM: ▪ https://thalesdocs.com/gphsm/luna/7/docs/pci/Content/install/client_install/software.htm ▪ https://thalesdocs.com/gphsm/luna/7/docs/pci/Content/admin_hsm/PED_Auth/PED_Auth.htm
P2-7	Physically secure 3DS systems	7.1 Data center security 7.2 CCTV	**Azure:** Azure maintains the physical security controls for Azure data centers and colocations supporting the services within the 3DE and meets the necessary 3DS requirements for their customers as noted within the PCI 3DS AOC. **Customers:** Azure customers are responsible for managing the physical security of systems not managed within the Azure environment. Azure customers are also responsible for

3DS PART 2 REQUIREMENTS			RESPONSIBILITY SUMMARY
			implementing and configuring MFA controls into telecommunications rooms hosted in their 3DE, as applicable.

Table 2: Azure PCI 3DS Part 2 Requirements Responsibility

SAMPLE IMPLEMENTATION OF ACS COMPONENT IN AN AZURE ENVIRONMENT

The below diagram demonstrates a sample use case scenario for a company that has implemented 3DS ACS within their Azure 3DE hosted environment. For this example, it is assumed that the ACS software vendor has developed ACS software and was sold to an end-user customer – in this instance, an issuer. ACS software is required to comply with the EMV 3DS 2.0 specification[8], Visa Security Requirements (PCI 3DS AOC), and Visa's 3DS 2.0 program[9] requirements prior to implementation of the ACS component by the issuer or issuer processor. For this sample use case scenario, it is also assumed that the ACS software is compliant with the EMV 3DS 2.0 specifications and Visa 3S 2.0 program requirements. The example company, Company ABC, is an online issuer company that performs 3DS functions within their 3DE that is hosted in the Azure cloud platform.

The ACS software is deployed within the Company ABC's Azure private cloud environment and integrated with their existing PCI DSS compliant environment, as shown in the sample 3DS diagram below.

[8] https://www.emvco.com/emv-technologies/3d-secure/

[9] https://technologypartner.visa.com/Library/3DSecure2.aspx

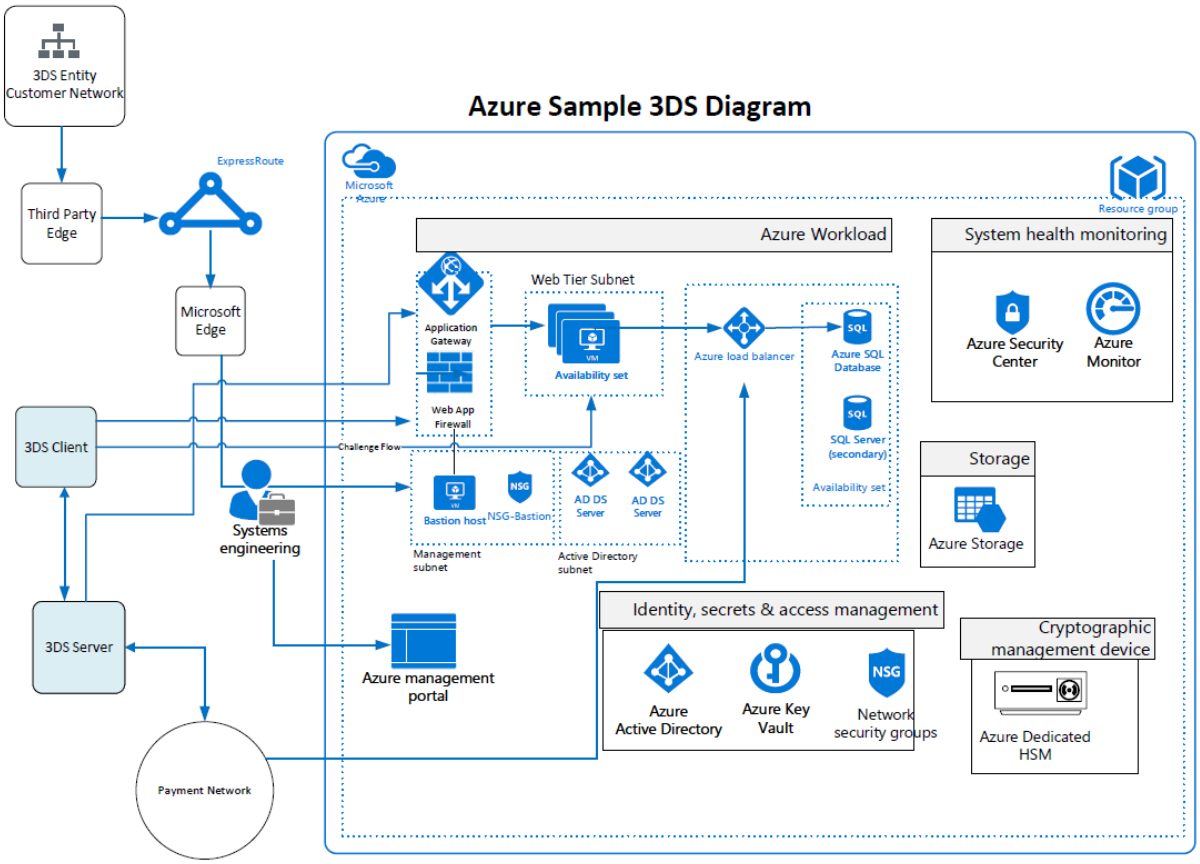

Figure 3: Sample 3DS Architecture Diagram for Company ABC

Figure 3 demonstrates a sample high-level architecture for the implementation of the 3DS ACS component in the Azure cloud platform. 3DS Part 2 requirements sections below describe how Company ABC could utilize various Azure services for their 3DE hosted on the Azure cloud platform to meet several controls identified within the 3DS Part 2 requirements P2-1 through P2-7.

REQUIREMENT P2-1: SCOPING

Company ABC integrated the 3DS ACS software and the necessary components within the Azure cloud platform. Azure 3DE provided the necessary segmentation in the cloud. Company ABC ensured that the traffic is managed with the 3DS components residing outside the 3DE. Identity, secrets, and access management services as shown in Figure 3 were configured by Company ABC to segment their 3DE.

REQUIREMENT P2-2: SECURITY GOVERNANCE

Company ABC identified and defined the security objectives, roles and responsibilities, risk management strategy, and third-party relationships procedures for their 3DE. The Azure policy service was configured to achieve governance for use of resources in the 3DE.

REQUIREMENT P2-3: PROTECT 3DS SYSTEMS AND APPLICATIONS

Company ABC identified the connections to be permitted within their 3DE network. Used network security group configurations for permitting and blocking access into the 3DE. The Azure application gateway was

used for managing traffic to the web applications in the 3DE. Azure AD solution was configured with features such as MFA and role-based access (with segment management group for limited access) for access into the 3DE. Azure AD monitoring was enabled for detecting and triggering alerts related to suspicious activities.

Azure VMs were configured to host the 3DS web application servers. Company ABC configured the necessary ACS software and Internet Information Services (IIS) web server software in accordance with guidelines from the software vendors and configured the VM per the guidelines from Azure to meet server hardening requirements. For the Azure Bastion Host, a secure VM was used for administering connections to other VMs. Azure VNet created subnets to provide isolation with the Azure cloud and for secure communication between Azure resources such as Azure VMs.

Azure load balancers were leveraged to manage outbound connections from the ACS server residing on the VM to other 3DS components outside the 3DE. Internal load balancers were also utilized to balance traffic inside the virtual network.

To manage the remote access and perform cryptographic operations on the Azure Dedicated HSM, Company ABC utilized the external ISO-13491-validated, non-console access solution specified within the HSM security policy. Company ABC managed all the 3DS sensitive authentication operations, cryptographic processes, and key management on the Azure Dedicated HSM.

REQUIREMENT P2-4: SECURE LOGICAL ACCESS TO 3DS SYSTEMS

Azure ExpressRoute created a private connection between Azure data centers and infrastructure hosted by Company ABC. Azure ExpressRoute enabled access to the Azure services hosted in the 3DE. MFA configured through Active Directory used password and an OATH hardware token as the two factors.

Azure Monitor monitored various resources, VMs, and applications within the 3DE and was used for analyzing the collected data. Alerts were configured to notify for any critical conditions. Azure AD monitoring also detected and triggered alerts for any suspicious actions related to access to 3DE.

REQUIREMENT P2-5: PROTECT 3DS DATA

Company ABC identified the various types of 3DS sensitive data, such as 3DS authentication data, authentication challenge data that is application- and browser-based and stored within the SQL database, as well as the data that is transmitted internally and externally to other 3DS components. Restrictions were enforced on the VMs and the systems storing sensitive data, including the Azure Dedicated HSMs that managed the keys protecting the 3DS sensitive data.

For Azure application gateways, Microsoft IIS servers were configured for the appropriate Transport Layer Security (TLS) 1.2 protocol and strong cipher suites.

REQUIREMENT P2-6: CRYPTOGRAPHY AND KEY MANAGEMENT

Company ABC utilized Azure Dedicated HSM for the management of cryptographic keys (symmetric keys, in this scenario) for the protection of 3DS sensitive data and used the Azure Dedicated HSM guidelines for provisioning the HSMs. The Azure Dedicated HSM was accessed using an Azure bastion dedicated for HSM operations. Company ABC utilized the HSM security policy to manage the cryptographic processes as intended along with use of a PED device for handling the cryptographic operations remotely when using a non-console access solution. Azure Security Center and Azure Monitor Services were used for capturing and monitoring the 3DS workload for analysis.

REQUIREMENT P2-7: PHYSICALLY SECURE 3DS SYSTEMS

Company ABC relies on Azure PCI DSS and 3DS compliance for physical security of 3DE in the Azure cloud. For systems not hosted in the cloud, Company ABC manages the physical security. Physical security is maintained for dedicated areas and rooms that provide non-console access to the Azure Dedicated HSMs hosed in the cloud.

CONCLUSION

Coalfire conducted PCI 3DS assessment for Azure cloud platform and validated it against the PCI 3DS Core Security Standard and PCI 3DS AOC can be retrieved from Azure compliance team. Azure maintains and manages its own compliance as part of its service provider responsibilities for the PCI 3DS Core Security Standard. 3DS entities that utilize Azure services must understand their responsibilities and the in-scope services that must be maintained and configured per the guidance from Azure 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 by the use of Azure services.

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

RESOURCES

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

- PCI 3DS Requirements: https://www.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss
- PCI DSS 3.2.1 Requirements: https://www.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss
- Azure Compliance – PCI DSS: https://docs.microsoft.com/en-us/compliance/regulatory/offering-pci-dss
- Azure Services Security Documentation: https://docs.microsoft.com/en-us/azure/security/
- Azure Security Fundamentals: https://docs.microsoft.com/en-us/azure/security/fundamentals/overview

ABOUT THE AUTHOR

Bhavna Sondhi | Principal

Bhavna Sondhi is the practice subject matter expert for the solution validation team at Coalfire. Bhavna performs advisory work and assessments for various PCI compliance frameworks and authors technical white papers. Bhavna joined Coalfire in 2013 and brings over 14 years of software engineering and information security experience to the team. Her software engineering experience plays a vital part in ensuring that the teams recognize the importance of secure code development and information security within their operational practices.

ABOUT THE REVIEWER

Eric Walker | Principal

Eric Walker is a Principal in the solution validation team with Coalfire. Eric has multiple years of experience working as a QSA (P2PE) and PA-QSA, helping clients develop systems and software for use in PCI DSS environments, and has authored and spoken on multiple security topics, including application security, social engineering, penetration testing, software development life cycle, security awareness, and PCI compliance. He holds QSA (P2PE), PA-QSA, GWAPT, CDPSE, CISSP, and ISO/IEC 27001:2013 Lead Auditor certifications.

Published 29 January 2021.

ABOUT COALFIRE

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