PCI PIN V3.1 ATTESTATION OF COMPLIANCE

PAYMENT CARD INDUSTRY PIN SECURITY STANDARD

Submitted to:

Microsoft Corporation - Microsoft Azure

Molly Bostic
Group Program Manager
One Microsoft Way
Redmond, WA, 98052

Submitted by:

Coalfire Systems, Inc.
Skyler Ferran
Principal
8480 E Orchard Rd., Suite 5800,
Greenwood Village, CO 80111

Management's Representation

Management of Microsoft Corporation has affirmed that all information provided to Coalfire Systems, Inc. (Coalfire) through interviews, documentation, walk-through descriptions, and observation, which serves as the basis for the scope, assessment and conclusions of this report is to the best of their knowledge accurate, complete and current as relates to requirements identified at the time of the assessment. Management of Microsoft Corporation further acknowledges that completion of this PCI PIN compliance validation assessment and a finding of compliant does not and will not prevent a potential compromise of key or PIN data on any Microsoft Corporation systems.

Confidential Information

This document contains confidential information relating to Microsoft Corporation. This is only documentation pertaining to an assessment and does not include professional services for remediation efforts. Information contained within this report is intended for the sole use of Microsoft Corporation, Coalfire, relevant Card Associations, and the Payment Card Industry Security Standards Council (PCI SSC).

Payment Card Industry (PCI)

PIN Security Requirements

Attestation of Compliance for Onsite Assessments

For use with PIN Security Requirements v3.1

Revision 1.0c

February 2023

Section 1: Assessment Information

Instructions for Submission

This Attestation of Compliance must be completed as a declaration of the results of the assessment of the subject entity compliance with the *Payment Card Industry PIN Security Requirements and Test Procedures* (PCI PIN). Complete all sections: The entity is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the entity requesting the assessment (e.g. Payment Brand) for reporting and submission procedures.

Part 1. Entity and Qualified PIN Assessor (QPA) Information

Part 1a. Entity Organization Information

Company Name:	Microsoft Corporation				
DBA (doing business as):	Microsoft Azure		Business Identifier:	N/A	
Contact Name:	Molly Bostic		Title:	Group Program Manager	
Telephone:	425-705-5104		E-mail:	mollybos@microsoft.com	
Business Address:	One Microsoft Way		City:	Redmond	
State/Province:	WA	Country:	USA	Postal Code:	98052
URL:	https://azure.microsoft.com/				

Part 1b. Qualified PIN Assessor Company Information (if applicable)

Company Name:	Coalfire Systems, Inc.				
Lead QPA Contact Name:	Skyler Ferran		Title:	Principal	
Telephone:	(877) 224-8077		E-mail:	sferran@coalfire.com	
Business Address:	8480 E Orchard Rd., Suite 5800		City:	Greenwood Village	
State/Province:	CO	Country:	USA	Postal Code:	80111
URL:	https://www.coalfire.com				

© 2019-2023 PCI Security Standards Council, LLC. All Rights Reserved.

Part 2. Executive Summary

Part 2a. Scope Verification

Services that were INCLUDED in the scope of the PCI PIN Assessment (check all that apply):

Type of service(s) assessed:

- ☐ PIN Acquirer Payment Processing - POS
- ☐ PIN Acquirer Payment Processing - ATM
- ☐ Remote Key Distribution Using Asymmetric Keys – Operations
- ☐ Certification and Registration Authority Operations
- ☐ Key-injection Facilities
- ☒ Others (specify): Azure Payment HSM (third-party service provider hosting HSMs)

***Note**: These categories are provided for assistance only, and are not intended to limit or predetermine an entity's service description. If you feel these categories don't apply to your service, complete "Others." If you're unsure whether a category could apply to your service, consult with the applicable payment brand.*

© 2019-2023 PCI Security Standards Council, LLC. All Rights Reserved.

Part 2a. Scope Verification *(continued)*

Services that are provided by the entity but were NOT INCLUDED in the scope of the PCI PIN Assessment (check all that apply):

Type of service(s) not assessed:

☐ PIN Acquirer Payment Processing - POS

☐ PIN Acquirer Payment Processing - ATM

☐ Remote Key Distribution Using Asymmetric Keys - Operations

☒ Certification and Registration Authority Operations

☐ Key-injection Facilities

☐ Other (specify):

Provide a brief explanation why any checked services were not included in the assessment:	Microsoft provides CA/RA services which are unrelated to signing of public keys for PIN processing entities; it is the responsibility of customers utilizing asymmetric keys in a PIN transaction processing environment to ensure any CA/RA is compliant to PCI PIN.

Part 2b. Locations

List types of facilities (for example, data centers, key-injection facilities, certification authority operations, etc.) and a summary of locations included in the PCI PIN review.

Type of facility assessed:	Date of Assessment	Location(s) of facility (city, country):
Data Centers Coalfire reviewed common enterprise security processes which are uniformly applied to all data centers, and sampled data centers of various region and classification to confirm implementation of all applicable logical and physical security controls.	04 Aug 2023 - 14 Aug 2023	**Amsterdam** West Europe **Ireland** North Europe **United States of America** Central US East US South Central US West US

Part 2c. Summary of Requirements Tested

For each PCI PIN Requirement, select one of the following:

- **Full** – The requirement and all sub-requirements of that requirement were assessed, and no sub-requirements were marked as “Not Tested” or “Not Applicable” in the ROC.

© 2019-2023 PCI Security Standards Council, LLC. All Rights Reserved.

- **Partial** – One or more sub-requirements of that requirement were marked as "Not Tested" or "Not Applicable" in the ROC.
- **None** – All sub-requirements of that requirement were marked as "Not Tested" and/or "Not Applicable" in the ROC.

For all requirements identified as either "Partial" or "None," provide details in the "Justification for Approach" column, including:

- Details of specific sub-requirements that were marked as either "Not Tested" and/or "Not Applicable" in the ROC
- Reason why sub-requirement(s) were not tested or not applicable

Note: *One table to be completed for each service covered by this AOC. Additional copies of this section are available on the PCI SSC website.*

Part 2c. Summary of Requirements Tested *(continued)*

PCI PIN Control Objective	Details of Control Objectives Assessed			
	Full	Partial	None	**Justification for Approach** (Required for all "Partial" and "None" responses. Identify which sub-requirements were not tested and the reason.)
Control Objective 1:	☐	☒	☐	Azure provides coverage for specified PCI PIN controls for the purpose of operating HSMs utilizing the Azure environment. Microsoft Azure is responsible for implementing the PCI PIN controls identified, as well as managing their own PIN compliance. Some PIN requirements must be met by sharing of responsibilities between the Azure customer and Azure; others may be satisfied by the customer's use of Azure services, while others may fall entirely to the customer to perform outside of Azure completely. Controls 1-1,1-2, 1-5, 2-1, 2-2, 2-3, 2-4, 3-1, 3-2, 3-3, 4-1 are fully a customer responsibility and are not applicable for Azure's PIN ROC testing.
Control Objective 2:	☐	☒	☐	Azure provides coverage for specified PCI PIN controls for the purpose of operating HSMs utilizing the Azure environment. Microsoft Azure customers are responsible for implementing the PCI PIN controls identified, as well as managing their own PIN compliance. Some PIN requirements must be met by sharing of responsibilities between the Azure customer and Azure; others may be satisfied by the customer's use of Azure services, while others may fall entirely to the customer to perform outside of Azure completely. 5-1.a is a partial responsibility shared with customer. Controls 6-1.1 through 6-1.5, 6-2, 6-3, 6-3.1 through 6-3.9, 6-4, 6-5, 6-6, 7-1, 7-2 are fully a customer responsibility and are not applicable for Azure's PIN ROC testing.
Control Objective 3:	☐	☒	☐	Azure provides coverage for specified PCI PIN controls for the purpose of operating HSMs utilizing the Azure environment. Microsoft Azure customers are

© 2019-2023 PCI Security Standards Council, LLC. All Rights Reserved.

Part 2c. Summary of Requirements Tested *(continued)*				
PCI PIN Control Objective	**Details of Control Objectives Assessed**			
	Full	**Partial**	**None**	**Justification for Approach** (Required for all "Partial" and "None" responses. Identify which sub-requirements were not tested and the reason.)
				responsible for implementing the PCI PIN controls identified, as well as managing their own PIN compliance. Some PIN requirements must be met by sharing of responsibilities between the Azure customer and Azure; others may be satisfied by the customer's use of Azure services, while others may fall entirely to the customer to perform outside of Azure completely. Controls 8-1, 8-2, 8-3, 8-4, 9-1, 9-2, 9-3, 9-4, 9-5, 9-6, 10-1, 10-2, 10-3, 10-4, 10-5, 11-1, 11-2 are fully a customer responsibility and are not applicable for Azure's PIN ROC testing.
Control Objective 4:	☐	☒	☐	Azure provides coverage for specified PCI PIN controls for the purpose of operating HSMs utilizing the Azure environment. Microsoft Azure customers are responsible for implementing the PCI PIN controls identified, as well as managing their own PIN compliance. Some PIN requirements must be met by sharing of responsibilities between the Azure customer and Azure; others may be satisfied by the customer's use of Azure services, while others may fall entirely to the customer to perform outside of Azure completely. Controls 12-1, 12-2, 12-3, 12-4, 12-5, 12-6, 12-7, 12-8, 12-9, 13-1, 13-2, 13-3, 13-4, 13-5, 13-6, 13-7, 13-8, 13-9, 14-1, 14-2, 14-3, 14-4, 14-5, 15-2, 15-3, 15-4, 15-5, 16-1, 16-2 are fully a customer responsibility and are not applicable for Azure's PIN ROC testing.
Control Objective 5:	☐	☒	☐	Azure provides coverage for specified PCI PIN controls for the purpose of operating HSMs utilizing the Azure environment. Microsoft Azure customers are responsible for implementing the PCI PIN controls identified, as well as managing their own PIN compliance. Some PIN requirements must be met by sharing of responsibilities between the Azure customer and Azure; others may be satisfied by the customer's use of Azure services, while others may fall entirely to the customer to perform outside of Azure completely. Azure provides coverage for specified PCI PIN controls for the purpose of operating HSMs utilizing the Azure environment. Microsoft Azure customers are responsible for implementing the PCI PIN controls identified, as well as managing their own PIN compliance. Some PIN requirements must be met by sharing of responsibilities between the Azure customer and Azure; others may be satisfied by the customer's use of Azure services, while others may fall entirely to the customer to perform outside of Azure completely.

© 2019-2023 PCI Security Standards Council, LLC. All Rights Reserved.

Part 2c. Summary of Requirements Tested *(continued)*				
PCI PIN Control Objective	**Details of Control Objectives Assessed**			
	Full	**Partial**	**None**	**Justification for Approach** (Required for all "Partial" and "None" responses. Identify which sub-requirements were not tested and the reason.)
				18-3 is a partial responsibility shared with customer. Controls 17-1, 18-1, 18-2, 18-4, 18-5, 18-6, 18-7, 19-1. 19-2, 19-3, 19-4, 19-5, 19-6, 19-7, 19-8, 19-9, 19-10, 19-11, 19-12, 20-1, 20-2, 20-3, 20-4, 20-5, 20-6 are fully a customer responsibility and are not applicable for Azure's PIN ROC testing.
Control Objective 6:	☐	☒	☐	Azure provides coverage for specified PCI PIN controls for the purpose of operating HSMs utilizing the Azure environment. Microsoft Azure customers are responsible for implementing the PCI PIN controls identified, as well as managing their own PIN compliance. Some PIN requirements must be met by sharing of responsibilities between the Azure customer and Azure; others may be satisfied by the customer's use of Azure services, while others may fall entirely to the customer to perform outside of Azure completely. Controls 21-1, 21-2, 21-3, 21-4, 22-1, 22-1.1 through 22-1.3, 22-2, 22-3, 22-4, 22-4, 23-1, 23-2, 23-3, 24-1, 24-2, 24-2.1 through 24-2.3, 25-1, 25-1.1 through 25-1.4, 25-2, 25-2.1, 25-3, 25-3.1 through 25-3.5, 25-4, 25-5, 25-5.1, 25-5.2, 25-6, 25-6.1 through 25-6.3, 25-7, 25-7.1, 25-7.2, 25-8, 25-8.1 through 25-8.9, 25-9, 26-1, 27-1, 27-2, 28-1, 28-2, 28-3, 28-4, 28-5, 28-5.1, 28-5.2 are fully a customer responsibility and are not applicable for Azure's PIN ROC testing.
Control Objective 7:	☐	☒	☐	Azure provides coverage for specified PCI PIN controls for the purpose of operating HSMs utilizing the Azure environment. Microsoft Azure customers are responsible for implementing the PCI PIN controls identified, as well as managing their own PIN compliance. Some PIN requirements must be met by sharing of responsibilities between the Azure customer and Azure; others may be satisfied by the customer's use of Azure services, while others may fall entirely to the customer to perform outside of Azure completely. Below controls are partially shared with customer, 29-1, 29-1.1, 29-1.1.1, 29-1.1.2, 29-1.2, 29-2 29-3, 31-1, 31-1.1 through 31-1.6, 32-1, 32-1.1 through 31-1.5, 33-1. Controls 30-1, 30-2, 30-3, 32-2.1, 32-2.2, 32-2.2.1 through 32-2.2.3, 32-2.3, 32-2.3.1, 32-2.3.2, 32-2.4, 32-2.5, 32-2.5.1, 32-2.5.2, 32-2.6, 32-2.6.1, 32-2.6.2, 32-2.7, 32-2.7.1 through 32-2.7.4, 32-2.8, 32-2.8.1, 32-2.9, 32-2.91 through 32-2.9.7, 32-3, 32-3.1, 32-3.2, 32-3.3, 32-2.4, 32-4, 32-4.1, 32-4.2, 32-5, 32-6, 32-6.1, 32-6.2, 32-6.3, 32-7, 32-7.1, 32-8, 32-8.1 through 32-8.7, 32-9,

© 2019-2023 PCI Security Standards Council, LLC. All Rights Reserved.

Part 2c. Summary of Requirements Tested *(continued)*				
PCI PIN Control Objective	**Details of Control Objectives Assessed**			
	Full	**Partial**	**None**	**Justification for Approach** (Required for all "Partial" and "None" responses. Identify which sub-requirements were not tested and the reason.)
				32-9.1, 32-9.2 through 32-9.12 are fully a customer responsibility and are not applicable for Azure's PIN ROC testing.
Annex A1 – Control Objective 3:	☐	☐	☒	N/A – Azure CA/RA services are not in scope for this assessment.
Annex A1 – Control Objective 4:	☐	☐	☒	N/A – Azure CA/RA services are not in scope for this assessment.
Annex A1 – Control Objective 5:	☐	☐	☒	N/A – Azure CA/RA services are not in scope for this assessment.
Annex A1 – Control Objective 6:	☐	☐	☒	N/A – Azure CA/RA services are not in scope for this assessment.
Annex A2 – Control Objective 3	☐	☐	☒	N/A – Azure RKD services are not in scope for this assessment.
Annex A2 – Control Objective 4:	☐	☐	☒	N/A – Azure RKD services are not in scope for this assessment.
Annex A2 – Control Objective 5:	☐	☐	☒	N/A – Azure RKD services are not in scope for this assessment.
Annex A2 – Control Objective 6:	☐	☐	☒	N/A – Azure RKD services are not in scope for this assessment.
Annex A2 – Control Objective 7:	☐	☐	☒	N/A – Azure RKD services are not in scope for this assessment.
Annex B – Control Objective 1:	☐	☐	☒	N/A – Azure is not a KIF
Annex B – Control Objective 2:	☐	☐	☒	N/A – Azure is not a KIF
Annex B – Control Objective 3:	☐	☐	☒	N/A – Azure is not a KIF
Annex B – Control Objective 4:	☐	☐	☒	N/A – Azure is not a KIF
Annex B – Control Objective 5:	☐	☐	☒	N/A – Azure is not a KIF
Annex B – Control Objective 6:	☐	☐	☒	N/A – Azure is not a KIF

© 2019-2023 PCI Security Standards Council, LLC. All Rights Reserved.

Part 2c. Summary of Requirements Tested *(continued)*				
PCI PIN Control Objective	**Details of Control Objectives Assessed**			
	Full	**Partial**	**None**	**Justification for Approach** (Required for all "Partial" and "None" responses. Identify which sub-requirements were not tested and the reason.)
Annex B – Control Objective 7:	☐	☐	☒	N/A – Azure is not a KIF

© 2019-2023 PCI Security Standards Council, LLC. All Rights Reserved.

Section 2: Report on Compliance

This Attestation of Compliance reflects the results of an onsite assessment, which is documented in an accompanying Report on Compliance (ROC).

The assessment documented in this attestation and in the ROC was completed on:	*08 Sep 2023*	
Have compensating controls been used to meet any requirement in the ROC?	☐ Yes	☒ No
Were any requirements in the ROC identified as being not applicable (N/A)?	☒ Yes	☐ No
Were any requirements not tested?	☐ Yes	☒ No
Were any requirements in the ROC unable to be met due to a legal constraint?	☐ Yes	☒ No

© 2019-2023 PCI Security Standards Council, LLC. All Rights Reserved.

Section 3: Validation and Attestation Details

Part 3. PCI PIN Validation

This AOC is based on results noted in the ROC dated *08 Sep 2023.*

Based on the results documented in the ROC noted above, the signatories identified in Parts 3b-3c, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document (***check one):***

☒	**Compliant:** All sections of the PCI PIN ROC are complete, all questions answered affirmatively, resulting in an overall **COMPLIANT** rating; thereby *Microsoft Azure* has demonstrated full compliance with the PCI PIN Security Requirements.
☐	**Non-Compliant:** Not all sections of the PCI PIN ROC are complete, or not all questions are answered affirmatively, resulting in an overall **NON-COMPLIANT** rating, thereby *(Service Provider Company Name)* has not demonstrated full compliance with the PCI PIN Security Requirements. **Target Date** for Compliance: An entity submitting this form with a status of Non-Compliant may be required to complete the Action Plan in Part 4 of this document. *Check with the payment brand(s) before completing Part 4.*
☐	**Compliant but with Legal exception:** One or more requirements are marked "Not in Place" due to a legal restriction that prevents the requirement from being met. This option requires additional review from acquirer or payment brand. *If checked, complete the following:*

Affected Requirement	Details of how legal constraint prevents requirement being met

Part 3a. Acknowledgement of Status

Signatory(s) confirms:

(Check all that apply)

☒	The ROC was completed according to the *PCI PIN Security Requirements and Testing Procedures*, Version *3.1*, and was completed according to the instructions therein.
☒	All information within the above-referenced ROC and in this attestation fairly represents the results of my assessment in all material respects.
☒	I have read the PCI PIN and I recognize that I must maintain PCI PIN compliance, as applicable to my environment, at all times.
☒	If my environment changes, I recognize I must reassess my environment and implement any additional PCI PIN requirements that apply.

© 2019-2023 PCI Security Standards Council, LLC. All Rights Reserved.

Part 3b. Assessed Entity PIN Security Attestation

Molly Bostic
Molly Bostic (Sep 8, 2023 11:17 PDT)

Signature of Executive Officer of Assessed Entity ↗	
Assessed Entity Executive Officer Name:	**Molly Bostic**
Title:	**Group Program Manager**
Date:	Sep 8, 2023

Part 3c. Qualified PIN Assessor (QPA) Company Acknowledgement

Describe the role performed by the QPA and others that participated from within the QPA Company:	*Assesor performed the site visits (virtual and physical), interviewed appropriate personnel, reviewed provided documentation and evidence, and documented the ROC and AOC*

Signature of Duly Authorized Officer of QPA Company ↗	*Date:* Sep 8, 2023
Duly Authorized Officer Name: Skyler Ferran	*QPA Company:* Coalfire Systems, Inc.

© 2019-2023 PCI Security Standards Council, LLC. All Rights Reserved.

Part 4. Action Plan for Non-Compliant Requirements

Select the appropriate response for "Compliant to PCI PIN" for each requirement. If you answer "No" to any of the requirements, you may be required to provide the date your Company expects to be compliant with the requirement and a brief description of the actions being taken to meet the requirement.

Check with the applicable payment brand(s) before completing Part 4.

PCI PIN Control Objective	Description of Control Objective	Compliant to PCI PIN Control Objective *(Select One)*		Remediation Date and Actions (If "NO" selected for any Control Objective
		YES	NO	
Control Objective 1:	PINs used in transactions governed by these requirements are processed using equipment and methodologies that ensure they are kept secure.	☒	☐	
Control Objective 2:	Cryptographic keys used for PIN encryption/decryption and related key management are created using processes that ensure that it is not possible to predict any key or determine that certain keys are more probable than other keys.	☒	☐	
Control Objective 3:	Keys are conveyed or transmitted in a secure manner.	☒	☐	
Control Objective 4:	Key-loading to HSMs and POI PIN-acceptance devices is handled in a secure manner.	☒	☐	
Control Objective 5:	Keys are used in a manner that prevents or detects their unauthorized usage.	☒	☐	
Control Objective 6:	Keys are administered in a secure manner.	☒	☐	
Control Objective 7:	Equipment used to process PINs and keys is managed in a secure manner.	☒	☐	
Annex A1 – Control Objective 3:	Keys are conveyed or transmitted in a secure manner.	☒	☐	
Annex A1 – Control Objective 4:	Key-loading to HSMs and POI PIN-acceptance devices is handled in a secure manner.	☒	☐	
Annex A1 – Control Objective 5:	Keys are used in a manner that prevents or detects their unauthorized usage.	☒	☐	
Annex A1 – Control Objective 6:	Keys are administered in a secure manner.	☒	☐	
Annex A2 – Control Objective 3	Keys are conveyed or transmitted in a secure manner.	☒	☐	

© 2019-2023 PCI Security Standards Council, LLC. All Rights Reserved.

PCI PIN Control Objective	Description of Control Objective	Compliant to PCI PIN Control Objective *(Select One)*		Remediation Date and Actions (If "NO" selected for any Control Objective
		YES	NO	
Annex A2 – Control Objective 4:	Key-loading to HSMs and POI PIN-acceptance devices is handled in a secure manner.	☒	☐	
Annex A2 – Control Objective 5:	Keys are used in a manner that prevents or detects their unauthorized usage.	☒	☐	
Annex A2 – Control Objective 6:	Keys are administered in a secure manner.	☒	☐	
Annex A2 – Control Objective 7:	Equipment used to process PINs and keys is managed in a secure manner.	☒	☐	
Annex B – Control Objective 1:	PINs used in transactions governed by these requirements are processed using equipment and methodologies that ensure they are kept secure.	☒	☐	
Annex B – Control Objective 2:	Cryptographic keys used for PIN encryption/decryption and related key management are created using processes that ensure that it is not possible to predict any key or determine that certain keys are more probable than other keys.	☒	☐	
Annex B – Control Objective 3:	Keys are conveyed or transmitted in a secure manner.	☒	☐	
Annex B – Control Objective 4	Key-loading to HSMs and POI PIN-acceptance devices is handled in a secure manner.	☒	☐	
Annex B – Control Objective 5:	Keys are used in a manner that prevents or detects their unauthorized usage.	☒	☐	
Annex B – Control Objective 6:	Keys are administered in a secure manner.	☒	☐	
Annex B – Control Objective 7:	Equipment used to process PINs and keys is managed in a secure manner.	☒	☐	

© 2019-2023 PCI Security Standards Council, LLC. All Rights Reserved.

FY24 Azure PCI PIN audit report

Final Audit Report 2023-09-08

Created:	2023-09-08
By:	Gavin Squire (gasquir@microsoft.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAACXUu5WZ1Yx6t3_z3aIXghCz1dRHfL6Nw

"FY24 Azure PCI PIN audit report" History

Document created by Gavin Squire (gasquir@microsoft.com)
2023-09-08 - 5:59:17 PM GMT- IP address: 172.83.6.13

Document emailed to Molly Bostic (mollybos@microsoft.com) for signature
2023-09-08 - 6:00:14 PM GMT

Document emailed to skyler.ferran@coalfire.com for signature
2023-09-08 - 6:00:14 PM GMT

Email viewed by Molly Bostic (mollybos@microsoft.com)
2023-09-08 - 6:09:51 PM GMT- IP address: 73.227.108.10

Document e-signed by Molly Bostic (mollybos@microsoft.com)
Signature Date: 2023-09-08 - 6:17:24 PM GMT - Time Source: server- IP address: 73.227.108.10

Email viewed by skyler.ferran@coalfire.com
2023-09-08 - 6:29:03 PM GMT- IP address: 71.214.64.7

Signer skyler.ferran@coalfire.com entered name at signing as Skyler Ferran
2023-09-08 - 6:29:31 PM GMT- IP address: 71.214.64.7

Document e-signed by Skyler Ferran (skyler.ferran@coalfire.com)
Signature Date: 2023-09-08 - 6:29:33 PM GMT - Time Source: server- IP address: 71.214.64.7

Agreement completed.
2023-09-08 - 6:29:33 PM GMT

Microsoft | Powered by Adobe Acrobat Sign