Visa PIN Security Program Guide

Visa Supplemental Requirements

Version 3.0

August 2019

Visa PIN Security Program Guide

Visa Supplemental Requirements

Version 3.0

August 2019

The information in this document is intended for use by Visa employees, Visa clients, and other external persons and entities that participate in the Visa PIN Security Program.

THIS DOCUMENT IS PROVIDED ON AN "AS IS", "WHERE IS", BASIS, "WITH ALL FAULTS" KNOWN AND UNKNOWN. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, VISA EXPLICITLY DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, REGARDING THE LICENSED WORK AND TITLES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT.

THE INFORMATION CONTAINED HEREIN MUST BE MAINTAINED IN ACCORDANCE WITH THE VISA CORE RULES AND VISA PRODUCT AND SERVICE RULES, THE INTERLINK NETWORK INC. OPERATING REGULATIONS, AND THE PLUS SYSTEM, INC. OPERATING REGULATIONS.

THIS PAGE INTENTIONALLY LEFT BLANK.

Contents

THIS PAGE INTENTIONALLY LEFT BLANK.

Change History

Date	Version	Section	Description
November 2015	1.0	All	Public versioning and consolidation of document • Updated document with latest program definitions • Clarified definitions of Validating and Non-Validating participants • Clarified that merchants who process PINs for Visa transactions are Non-Validating participants • Enhanced description of Encryption and Support Organizations (ESO)
May 2017	1.1	Appendix B	Update Appendix B, to reflect v5 POI dates
July 2018	2.0	All	Updates to reflect Europe region PIN Program Integration
August 2019	3.0	All	Updates to reflect transition from Visa Approved PIN Assessors to PCI Qualified PIN Assessors (QPA)

THIS PAGE INTENTIONALLY LEFT BLANK.

About This Guide

The Visa PIN Security Program Guide outlines the security and procedural requirements for acquirers and/or their agent(s) who handle or manage PIN data or are involved with key management that protect PINs associated with Visa transactions.

This program guide is applicable to all Visa Inc. operating regions: Asia-Pacific (AP), Canada, Central and Eastern Europe, Middle East and Africa (CEMEA), Europe, Latin America and Caribbean (LAC) and United States (U.S.).

Visa may change and add to this material as needed to address potential threats, vulnerabilities, or updates.

The Visa PIN Security Program is administered by Visa's Global Risk team.

Note: This document is a supplement to the *Visa Core Rules and Visa Product and Service Rules*, the *Interlink Network Inc. Operating Regulations*, and the *Plus System, Inc. Operating Regulations*. In the event of any conflict between any content in this document, any document referenced herein, any exhibit to this document, or any communications concerning this document, and any content in the *Visa Core Rules and Visa Product and Service Rules*, the *Interlink Network Inc. Operating Regulations*, and *Plus System, Inc. Operating Regulations*, the *Visa Core Rules and Visa Product and Service Rules*, the *Interlink Network Inc. Operating Regulations*, and the *Plus System, Inc. Operating Regulations*, shall govern and control.

Intended Audience

The intended audiences of this document are all organizations involved with handling Visa PIN data, whether it involves PIN processing, translation, acceptance and/or key management, management or security of these environments. Organizations include but are not limited to:

- Visa PIN Security Program administrators
- PCI Qualified PIN Assessor (QPA)*
- All organizations that accept and process Visa, Plus, Interlink, or Electron PINs
- All organizations that perform key management activities in support of PIN processing
- All organizations that manage or deploy PIN acceptance devices that process and accept cardholder PINs at Automated Teller Machines (ATM), Point of Sale (POS) terminals, or kiosks (i.e. encryption support organizations, key injection facilities)
- Financial institutions or merchant banks (also known as sponsoring acquirers) that register third party agents

* Visa Approved PIN SA are recognized by the Visa PIN Security Program until 1 October 2019.

Related Publications

The following additional documents and website are to be used in support of the Visa PIN Security Program:

- Payment Card Industry PIN Security Requirements and Assessment Procedures https://www.pcisecuritystandards.org/security_standards/documents.php Filter by PTS
- Payment Card Industry Transaction Security (PTS) Point of Integration Security Requirements https://www.pcisecuritystandards.org/security_standards/documents.php Filter by PTS
- Payment Card Industry Transaction Security Hardware Security Module Security Requirements https://www.pcisecuritystandards.org/security_standards/documents.php. Filter by PTS
- Payment Card Industry Software-based PIN Entry on Commercial Off the Shelf (COTS) Security Requirements https://www.pcisecuritystandards.org/security_standards/documents.php. Filter by SPOC
- Visa PIN Entry Device (PED) Requirements https://usa.visa.com/dam/VCOM/global/partner-with-us/documents/visa-ped-requirments.pdf)
- Visa PIN Security Website www.visa.com/pinsecurity

For More Information

For more information about the Visa PIN Security Program, contact your regional Visa program manager:

AP and CEMEA:	pinsec@visa.com
Europe	visaeuropepin@visa.com
LAC:	pinlac@visa.com
North America:	pinna@visa.com
Global:	pin@visa.com

Authority

The *Visa PIN Security Program Guide* outlines the security and procedural requirements for organizations processing PIN data associated with Visa cards or performing key management to support PIN processing. Visa Risk administers this program.

Visa may change and add to this material as needed to address potential threats, vulnerabilities, or updates.

Introduction

The Importance of PIN Security

The Personal Identification Number (PIN) is a Cardholder Verification Method (CVM) used to verify the cardholder at the point of transaction. The value of the PIN as a means of verifying the identity of the cardholder is dependent exclusively on the secrecy of the PIN from the moment it is created, to the instant it is entered into the interchange system, and through the issuer verification process. Card issuers expect that their customer PINs will be protected through the interchange process, while the acquirers depend on consumer confidence to facilitate their desired transaction volume. Failure to adhere to the requirements increases the risk of compromise, resulting in monetary losses related to the investigation of fraud claims and the erosion of consumer confidence in the payment system.

Ensuring the confidentiality of cardholder PINs throughout the interchange cycle requires adherence to a set of globally recognized security requirements. Basic to these standards is the cryptographic protection of cardholder PINs. Such protection requires the implementation of specific controls to assure that the intended level of security is achieved by all participants.

The successful management of payment system risks depends on the cooperation of all participants in the payment ecosystem. There must be reasonable assurance that a cardholder PIN will not be compromised when used in the Automated Teller Machines (ATM)/cash dispensers or the Point of Sale (POS) devices when in the control of other networks and service providers.

PIN Security Program Background

Visa is committed to protecting the Visa payment system and sensitive data that flows through the network. This includes Visa cardholder PIN data. Visa created the PIN Security Program outlining security and compliance validation requirements with that acquirers and/or their third party agents must follow.

Visa PIN Security Program requirements include:

- PCI PIN Security Requirements
- Visa PIN Entry Device (PED) Hardware Requirements
- Visa TDES Requirements
- Visa Software-based PIN Entry Solutions Requirements

Adherence to these requirements results in more than simply securing PIN data. Sound security practices help to protect organizations from adverse financial and reputational consequences often associated with PIN data compromises and fundamentally ensures that cardholder confidence in the payment ecosystem is preserved.

PIN Security Program Objectives

Visa's PIN Security Program establishes a global framework to support:

- Consistent risk based approaches to identify Visa PIN Security Program participants
- Common validation requirements

The PIN Security Program is based on the current risk environment that exists for Visa cardholder PINs. Visa will inform clients of any changes to the PIN Security Program based on exploited vulnerabilities, emerging risks, and threats to the payment system.

Visa Core Rules and Visa Product and Service Rules

The Visa PIN Security Program is supported by the following Visa Rules:

- Rule ID# 0000708 - PIN Security Indemnification
- Rule ID# 0001288 - PIN Security Non-Compliance Assessments
- Rule ID# 0008138 - ATM Operator and Agent Requirements
- Rule ID# 0026001 - Data Compromise Recovery
- Rule ID# 0027086 - Visa PIN Security Program Requirements

For details on these and other Visa Rules, visit www.visa.com

PIN Security Program Fees

There are no program fees associated with the Visa PIN Security Program.

Any professional fees and expenses associated with onsite PIN security assessments must be settled between the PIN participant and the security assessor.

Roles and Responsibilities

The success of PIN security depends on the cooperation of all stakeholders, who must be aware of and understand their responsibility to secure PIN data.

The following section describes the Visa PIN Security Program Stakeholders and their responsibilities.

PIN Program Participants

PIN Security Program participants are acquirers, their merchants and/or their third party agent(s) who process PINs for Visa transactions, provide key management functions or support PIN entry devices.

All PIN Security Program participants must comply with the security requirements specified in this guide.

There are two categories of PIN Security Program Participants, Validating Participants and Non-Validating Participants. Refer to Program Framework Components of this guide for additional information.

Sponsoring Acquirers

These are Visa Acquirers who engage, either directly or indirectly, with third party service providers that handle Visa PIN data, including PIN processing, translation, acceptance and/or key management on their behalf. Their responsibilities include:

- Ensure all third party agents are properly registered with Visa using the Program Request

Management tool (PRM)

- Perform due diligence prior to engaging any third party agent and ensuring policies and procedures are in place to provide the correct level of oversight and control of the third party agent regarding the Visa PIN Security Program
- Ensure Third Party Agents that acquire and process PIN data or perform key management functions in support of PIN processing are PCI PIN compliant and adhere to the Visa Rules.

If the third party agent is contracted by the acquirers' merchant or Independent Sales Organization (ISO), the acquirer remains responsible to conduct the appropriate PIN security due diligence and ensure that the merchant/ISOs and their third party agents comply with the relevant Visa and industry requirements.

Visa

As the steward of the Visa PIN Security Program, the Visa Risk team's responsibilities include:

- Administer the Visa PIN Security Program Framework
- Maintain the Visa PIN Security Program Guide
- Manage and publish Visa PIN Entry Device (PED) Hardware Requirements
- Manage regional compliance programs that:
    - Track the Validating Participants' compliance validation
    - Identify new Validating Participants
    - Communicate applicable security requirements and answer queries relating to PIN Security Program requirements
    - Update the Global Registry of Service Providers with Validating Participants that have successfully demonstrated their compliance to the Visa PIN Security Program requirements
- Respond to questions relating to compliance validation requirements

PCI Qualified PIN Security Assessors (QPA)

These are experienced security professionals who are listed and approved by the PCI SSC as qualified to perform security assessments against PCI PIN Security Requirements in support of the Visa PIN Security Program.

Effective 1 October 2019, all onsite PIN assessments must be performed by an approved and listed PCI QPA. PIN assessments that are in progress or scheduled but will not be performed until after 1 October 2019, may continue to use a Visa Approved PIN Assessor that is not a QPA. In these cases, Visa approval is required prior to the assessment taking place. Contact the regional PIN Program Manager for additional information. This exception is only allowed for assessments performed between 1 October 2019 through 31 December 2019. *Effective 1 January 2020, all onsite PIN assessments must be performed by an approved PCI QPA.*

QPA responsibilities include:

- Directly contract with the Validating Participant to perform an onsite assessment
- Schedule, plan, and perform onsite PIN security assessments
- Release assessments and remediation reports to Validating Participants upon completion of onsite assessments
- Validate all remediation activities with the organization, including follow-ups and evidence reviews to ensure any non-compliance issues have been resolved
- Provide Visa with the PCI PIN Reporting of Compliance (ROC) and PCI PIN Attestation of Compliance (AOC) when the Validating Participant has achieved full compliance with the applicable security requirement(s)
- Contact the PCI SSC for any questions relating to PCI standards or FAQs

A PCI QPA Company and individual QPA may not assess the same organization for more than two consecutive review cycles unless approved or specifically directed by Visa.

Payment Card Industry Security Standards Council (PCI SSC)

As the steward of the PCI Security Standards, the PCI SSC responsibilities include:

- Manage and update PCI Security Requirements associated with the PIN Program, including publishing FAQs and related program materials,
- Train, certify and list approved QPA companies and individual QPAs on the PCI website
- Respond to questions pertaining to PCI standards

Any questions specific to the requirements should be sent directly to PCI SSC using the following email: pcipts@pcisecuritystandards.org

Program Framework Components

Visa's PIN Security Program consists of five components that include:

1. PIN Security Program Participants
2. PIN Security Program Requirements
3. Qualified PIN Assessors (QPA)
4. Third Party Agent Program
5. PIN Security Program Compliance Enforcement

PIN Security Program Participants

Validating Participants

These are organizations who act as service providers that handle Visa PIN data, including PIN processing, translation, acceptance and/or perform key management to support PIN services on behalf of Visa clients.

Validating Participants must fully comply with the Visa PIN Security Program security and validation requirements described in this guide.

Organizations identified as Validating Participants must validate their PIN security compliance to Visa according to the requirements outlined in this program guide. Validating Participants are defined as:

- PIN Acquiring Third-Party VisaNet Processor (VNP) – A third party VNP entity that is directly connected to VisaNet and provides acquiring PIN processing services to Visa clients
- PIN Acquiring Client VNP acting as a Service Provider – A Visa client or client-owned entity that is directly connected to VisaNet and provides PIN acquiring processing services to Visa clients
- PIN Acquiring Third-Party Servicers (TPS) – A third-party agent that stores, processes, or transmits Visa account numbers and PINs on behalf of Visa clients
- Encryption and Support Organizations (ESO) – Organizations that:
  - Perform cryptographic key management services (i.e., key injection facilities (KIFs), Remote Key Injection (RKD) on behalf of Visa clients
  - Service and/or deploy client ATM, POS, or kiosk PIN entry devices (PEDs) which

process and accept cardholder PINs

- PED manufacturers and third party Certificate Authorities that manage various cryptographic key management responsibilities for clients

Other third party entities not specifically identified above that perform PIN translation, key management, and/or manage ATM or POS devices for Visa clients may be subject to the Visa PIN Security Program Requirements and classified as Validating Participants.

Note: PCI Software-based PIN Entry Solution providers are not considered Validating PIN Participants and not subject to Visa PIN Security Program. The PCI SSC manages the evaluation, testing and approval of software-based PIN entry solutions and lists approved solutions on their Approved Solutions website.

Contact your regional Visa Risk Representative for additional information on the applicability to your organization.

Validating Participants Compliance Requirements

- Perform an onsite PIN security assessment once every 24 months
- Onsite PIN security assessments must be performed by a PCI QPA identified on the PCI Qualified Assessor list
- Contract directly with a PCI QPA for the onsite PIN security assessment services
- Validating Participants must not use the same QPA individual or company for more than two (2) validation cycles unless approved or specifically directed by Visa
- Provide the QPA the necessary information to validate compliance with the applicable security requirement(s) before, during, and after (if needed) the onsite security assessment
- QPA results are provided to the Validating Participant stating a compliant or non-compliant status
- Validating Participant must resolve non-compliance issues within specified timeframes
- The QPA must verify remediation work to ensure compliance
- Remediation should be completed within 180 days after the final report is issued. Notify Visa if remediation extends beyond this period
- The QPA will send the PIN Attestation of Compliance (AOC) to Visa, indicating the Validating Participant's compliance with Visa's PIN Security Program requirements. The AOC must be signed by the Validating Participant executive management and the QPA

Non-Validating Participants

Visa clients, merchants and other organizations that acquire PIN transactions and/or perform key management services for only their own acquiring business are considered non-validating participants.

Non-validating participants must fully comply with the Visa PIN Security Program security requirements but validation requirements are different than Validating Participants. Non-Validating Participants must perform appropriate due diligence to ensure compliance with the PIN Security requirements in this document. This may include performing self-assessments using an internal or external resource. Individuals performing the self-assessment must have adequate knowledge of the PCI PIN Security Requirements, but do not need to be a QPA.

Self-assessment results do not need to be submitted to Visa but must retained as evidence of compliance. Visa reserves the right to request evidence of PIN compliance at any time or request an on-site PIN Security review of any organization, at any time, to ensure the security of the payment system.

Non-Validating participants should use the PCI PIN Report of Compliance template as a tool to assist with their validation efforts.

Visa reserves the right to re-categorize Non-Validating Participants as Validating Participants that must demonstrate compliance according to requirements outlined in this program guide.

Contact your regional Visa Risk Representative for additional information on applicability to your organization.

PIN Security Program Requirements

PCI PIN Security Requirements and Reporting and Validation Documents

The PCI PIN Security Requirements contain a complete set of controls for the secure management, processing, and transmission of personal identification number (PIN) data during online and offline payment card transaction processing at ATMs and attended and unattended point-of-sale (POS) terminals.

The requirements include:

- Identifying minimum security requirements for PIN-based interchange transactions
- Outlining the minimum acceptable requirements for securing PINs and encryption keys
- Assisting all retail electronic payment system participants in establishing assurances that cardholder PINs will not be compromised.

They also include specific requirements for entities involved in the implementation of symmetric key distribution using asymmetric keys (remote key distribution) or those entities involved in the operation of Certification Authorities.

The PCI PIN Requirements and associated reporting and validation materials are maintained by PCI Security Standards Council and are found on the PCI SSC website: www.pcisecuritystandards.org - PCI Standards & Documents > Documents Library> Filter by PTS.

Visa PIN Entry Device (PED) Hardware Requirements

PIN Security Program Participants must deploy and use PIN entry devices that are PCI PTS Approved and listed on the PCI Approved Device List.
https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices

In addition, PIN Security Program Participants must adhere to Visa PIN Entry Device (PED) requirements. These requirements assist organizations in their PED purchasing, usage and deployment strategies and help organizations protect themselves against PIN compromises, cardholder PIN data breaches, fraud, and ensures confidentiality and integrity of PIN data.

Additional information on Visa PED Hardware Requirements are found in Appendix B of this program guide or on the PIN security website, www.visa.com/pinsecurity.

Visa Triple Data Encryption Standard (TDES)

Visa's Triple Data Encryption Standard (TDES) requirements are:

- All ATMs must use TDES to protect pins
- All POS PIN acceptance devices must use TDES to protect pins.

U.S. only: Automated fuel dispensers (AFDs) must use TDES or Single DES Derived Unique Key per transaction (SDES DUKPT) to protect PINs. Sunset date for SDES DUKPT is 1 October 2020.

Visa Software-based PIN Entry Solution Requirements

Acquirers and their merchants deploying Software-based PIN Entry Solutions for payment acceptance must use solutions that have been validated and listed on the PCI SSC Approved Solution website. *https://www.pcisecuritystandards.org/assessors_and_solutions*

Qualified PIN Assessors (QPA)

Onsite PIN security assessments must only be performed by qualified personnel, therefore Visa requires that all onsite PIN assessments be performed by a QPA. The PCI QPA program ensures that PIN assessors have the required knowledge, skills, and experience in payment system security and the applicable PIN security requirements.

Onsite PIN Security Assessment Fees

Any professional fees and expenses associated with onsite assessments must be settled between the Validating Participant and the QPA.

List of PCI QPAs

Validating Participants must refer to the PCI Approved Assessor List to engage and contract directly with QPAs for onsite PIN assessments.

Approved QPAs are managed and listed by the PCI SSC and can be viewed at https://www.pcisecuritystandards.org/assessors_and_solutions/qpa_assessors. Questions about the QPA list can be directed to the PCI SSC.

Third Party Agent Program

Agent Registration

Third party agents that acquire and process or transmit PIN data, and Encryption Support Organizations (ESOs) that perform key management functions are considered Validating Participants and must be validated with an onsite assessment according to the Visa PIN security program requirements before they are registered with Visa.

Registration must be received by Visa via the Program Request Management (PRM) application. This online tool serves as the central location where clients can register third party agents and manage their relationships with these entities. For more information on Agent Registration, clients should visit http://www.visa.com/third-party-agent.

After the initial registration and validation, clients must ensure agents defined as Validating Participants continue to validate their Visa PIN Security Program compliance status with Visa every 24 months.

Third Party VisaNet Processors (VNPs)

A client that uses a VisaNet Processor, whether or not the VisaNet Processor is itself a client, must submit to Visa a VisaNet Processor and Third Party Registration and Designation (Exhibit 5E) form before using the VisaNet Processor. A Visa client that uses a non-client as a VisaNet Processor must ensure that the non-client submits to Visa a VisaNet Letter of Agreement (Exhibit 5A) before using the non-client as a VisaNet Processor. The Third Party Agent Program and VisaNet Processor program are separate and distinct Visa programs.

Onsite PIN assessments are required for all VisaNet processors that will be deploying PIN acquiring support for the first time.

Contact your regional Visa Risk Representative for additional information on requirements for new organizations.

Global Registry of Service Providers

Validating Participants who have successfully demonstrated compliance by submitting their PIN AOC to Visa will be listed on the Global Registry of Service Providers located on the Visa Service Provider website, www.visa.com/splisting. The registry is updated at the end of each month.

The *Global Registry of Service Providers* is a public website that serves as a platform where PIN Participants can broadcast their compliance with the Visa PIN Security Program. This important communication channel allows the PIN Participants to promote their services to potential clients worldwide and differentiate themselves as an organization that has demonstrated its commitment to security. The *Global Registry of Service Providers* website can be accessed at www.visa.com/splisting.

The registry also serves as a vehicle for all payment stakeholders to identify and ensure PIN Participants have met and comply with Visa security requirements. PIN Participants can use the registry to identify when compliance validation requirements must be satisfied.

Please note, that Visa reserves the right to remove any Validating Participant from the registry at its discretion.

PIN Security Program Compliance Enforcement

Visa maintains a global compliance program to ensure that the payment ecosystem is protected according to requirements of the PIN Security Program. All PIN Program Participants are required to comply with Visa PIN Security Requirements. Examples of non-compliance include, but are not limited to:

- Failure to comply with requirements defined in this program guide
- Failure to comply with specified security requirements
- If applicable, failure to remediate non-compliant findings
- Validating Participants failure to submit compliant Visa Attestation of Compliance by the required validation due date posted on the Visa Global Registry (https://www.visa.com/splisting/)

Compliance Validation Deadlines

Validating Participants are required to perform an onsite PIN security assessment once every 24 months. Thirty (30) days before the validation due date, Visa will send a reminder to the contact on file that your organization's validation is expiring. Upon expiration and if your organization is listed on the Visa Global Registry of Service Providers ("Registry"), your overdue validation status will be highlighted.

Validating Participants must submit a completed and signed PIN AOC before the participant is added to the Global Registry.

Failure to demonstrate compliance may result in a non-compliance assessment being issued to banks/financial institutions that use non-compliant service providers.

If Visa does not receive the appropriate revalidation documents:

- Within 1 - 60 days upon expiry of the validation documents, the PIN Participant will be highlighted in Yellow on the Registry.
- Within 61 - 90 days upon expiry of the validation documents, the PIN Participant will be highlighted in Red on the Registry.
- After 90 days, the PIN Participant will be removed from the Registry.

Validating Participants are encouraged to schedule their onsite PIN security assessment with sufficient time to prepare, perform the onsite PIN security assessment, and if required, remediate any non-compliant findings to ensure Visa receives the PIN AOC by the validation deadline.

Managing Non-Compliance

Visa encourages clients to immediately work with their PIN Security Program participants who are:

1. Non-compliant with Visa PIN Security Program and/or PCI PIN Security Requirements
2. Overdue on completing their compliance validation
3. Have never performed an onsite security review

In these cases, clients must submit at least one of the following on behalf of their validating participants:

- PIN Attestation of Compliance (AOC) – The PCI attestation form indicating the participant is compliant with Visa PIN Security program requirements
- Remediation Plan - Documented remediation plan that identifies areas of non-compliance and the action plan that describes when non-compliance will be corrected. Remediation plans should be completed within 180 days after the onsite assessment concludes.

Non-Compliance Assessments

Non-compliance assessments may be assessed for failure to comply with any Visa PIN Security Program Requirements specified in this program guide and/or applicable security requirements including:

- PCI PIN Security Requirements
- Visa PIN Entry Device (PED) Hardware Requirements
- Visa Triple DES Requirements
- Use of a PCI approved Software-based PIN Entry Solution

A Visa client may be subject to a non-compliance assessment for its or its agent's failure to comply with any of the requirements in the PIN Management Requirements Documents and Visa PIN Security Program Guide.

Currently, non-compliance assessments are levied as specified in the tables below. Visa reserves the right to levy non-compliance assessments as specified in the Visa Rules.

Violation	Non-Compliance Assessment
Initial violation and each month of unaddressed violations, up to 4 months after the initial violation	USD 10,000 per month
Violations after 4 months and each month thereafter	USD 25,000 per month

Clients that are subject to non-compliance assessments will receive detailed notifications itemizing the assessment amounts for the PIN Participant that they have sponsored.

Appendix A – Onsite PIN Security Assessment Process

Preparing for the PIN Assessment Review

It is important to gather the following information and have answers to the questions below before commencing a PIN security onsite assessment. QPAs will require at a minimum:

- Organization chart, listing the key management team members or participants
- Updated diagram flow of acquired PINs, PIN blocks, and encryption keys from any point of entry through the point of exit (identify all points, which cryptographically process or record PIN or key information). Ensure to include: key management methodology (master key/session key, connection with other entities, and translation points)
- Location(s) of facilities that perform cryptographic functions such as PIN translation, processing, verification and key storage, key creation, key injection/loading, as well as backup storage of cryptographic key materials
- Vendor product information for installed software that supports PIN environment and interchange processing
- Key inventory/key matrix
- Inventory of Encrypting PIN Pads (EPP) automated teller machines (ATM), cash dispensers, kiosks, automated fuel dispensers (AFD), and point of sale (POS) terminals with PIN pads; including device type and locations, with the PCI PTS approval numbers (firmware version, application version, etc.)
- Inventory of secure cryptographic devices (SCD), including hardware (host) security module (HSM)
- List of operating parameters (such as allowing single-length keys) enabled at SCDs
- Purchase orders for applicable SCDs and PEDs
- HSM command sets in use
- Total number of devices that are compliant with PCI PTS Device Security Requirements (Point of Interaction (POI) Modular Security Requirements)
- Total number of devices that are compliant with Visa PIN Entry Device Requirements and TDES mandates
- Key custodian agreements
- Documented procedures to support:

- Key generation
- Key storage
- Key loading
- Key distribution/conveyance
- Key destruction
- Key compromise
- Compliance of cryptographic tools and devices
- Device commissioning/decommission

Onsite PIN Security Assessment Methodology

The QPA will follow the Visa onsite PIN security assessment methodology that will include the following phases:

Phase	*Description*
Scope	• Identify the organization, services, processes and specific systems to be reviewed • QPA will evaluate scope of review and communicate to the Validating Participant the expected duration of the review
Planning	• Initial contact with the organization and obtain review confirmation • Confirm the type of organization being reviewed • Location and facilities to be reviewed (multi-site, third party sites) • Timeframe of the review
Data Gathering	• Obtain pre-site visit materials for the onsite security assessment (e.g. flow charts, policies, procedures, network diagrams, program questionnaires) • Pre-site visit materials and documents should be obtained prior to visiting site • Identify the lists of individuals/areas to be reviewed and obtain applicable documentation • Establish onsite agenda

Assessing of Internal Controls	• Review and evaluate the effectiveness of internal controls to the applicable security requirements • Obtain necessary quantitative and qualitative samples • Identify the areas of non-compliance
Communicating with Validating Participant's Management	• Conduct the exit interview with Senior Management of the organization (CEO/CFO or appointed representative of the Visa PIN Security Program participant)
Reporting	• Document and distribute the final report to the Validating Participant • Securely manage and retain working papers and reports per contract with Validating Participant
Follow-Up	• The QPA will track the Validating Participant's action plan to ensure remediation of non-compliance findings and overall compliance status • The QPA provides final compliance status to Visa using PCI PIN AOC that must be signed by the Validating Participant executive management and the QPA

Onsite PIN Security Assessment Duration

Duration for an onsite PIN security assessment will vary based on complexity of the Validating Participant's environment and services under review. Typical onsite PIN assessments can be one or two days in duration. Contact your QPA for more information about the onsite assessment process.

Appendix B – Visa PED Hardware Requirements

PED Hardware Purchase, Usage and Sunset Dates

Visa may revise PED Requirements based on evolving threats to the payment ecosystem.

Contact your regional Risk Representative for additional information.

Lab Evaluation Status	PED Type	PED Expiration Date	Purchase Requirements	Deployment Requirement*	Usage Requirement	Sunset / Retire Mandates
Devices never lab evaluated by Visa or PCI	Attended POS PED	–	Not allowed	Not allowed		July 31, 2010
	EPP used in Unattended POS / ATM / Kiosk	–	Not allowed	Not allowed	Allowed if device has not been moved prior to Oct 2005	Phase out devices with TDES/EMV conversions *Europe Region: Devices must be retired by December 31, 2020*
Pre-PCI Approved	Attended POS PED	Dec 31, 2007	Not allowed after device expiration date	Not allowed after sunset mandate	Not allowed after sunset mandate	Dec. 30, 2014 *Europe Region: Devices must be retired by December 31, 2012*
	EPP used in Unattended POS / ATM / Kiosk	Aug 31, 2008		Not allowed after device expiration date	Allowed if device has not been moved prior to Aug 2008	Phase out devices with TDES/EMV conversions *Europe Region: Devices must be retired by December 31, 2020*
PCI PED or EPP PED V1.X	Attended POS PED EPP used in Unattended POS / ATM / Kiosk	April 30, 2014	Not allowed after device expiration date	Allowed if purchased prior expiration date. *Europe Region: Deployment is not allowed after device expiration date*		Recommend device replacement *Europe Region: Attended/Semi-Attended devices must be retired by December 31, 2017. EPP used in unattended must be retired by December 31, 2020*
PCI PED or EPP PED V2.X	Attended POS PED EPP used in Unattended POS / ATM / Kiosk	April 30, 2017	Not allowed after device expiration date	Allowed if purchased prior expiration date.		Recommended device replacement *Europe Region: EPP used in unattended TBD- Under evaluation*
PCI PTS POI V3.X	Attended POS PED EPP used in Unattended POS / ATM / Kiosk	April 30, 2020	Not allowed after device expiration date	Allowed if purchased prior expiration date.		TBD - Under evaluation
PCI PTS POI V4.X	Attended POS PED EPP used in Unattended POS / ATM / Kiosk	April 30, 2023	Not allowed after device expiration date	Allowed if purchased prior expiration date.		TBD - Under evaluation
PCI PTS POI V5.X	Attended POS PED EPP used in Unattended POS / ATM / Kiosk	April 30, 2026	Not allowed after device expiration date	Allowed if purchased prior expiration date.		TBD - Under evaluation

Note: PEDs in the Europe Region formerly covered by the Semi-Attended environment definition are now governed by the requirements for the Attended environment