Payment Card Industry (PCI)
Data Security Standard

PFI PIN Security Requirements

Template for PFI PIN Security Requirements Report

Version 1.0

August 2014

Document Changes

Date	Version	Description
August 2014	1.0	To introduce the template for submitting PIN Security Requirements Report

Instructions for the Template for PFI PIN Security Requirements Report

This reporting template provides reporting tables and reporting instructions for PFIs to use, and should be completed fully. This can help provide reasonable assurance that a consistent level of reporting is present among PFIs. Do not delete any sections or rows of this template, but feel free to add rows as needed.

Use of this Reporting Template is mandatory for all PFI PIN Security Requirements Reports.

Objective		In Place		Cause of breach?		Contribute to breach?		Forensic Findings
		Yes	**No**	**Yes**	**No**	**Yes**	**No**	
Objective 1:	*PINs used in transactions governed by these requirements are processed using equipment and methodologies to ensure that they are kept secure.*							
1.	All cardholder-entered PINs are processed in equipment that conforms to the requirements for tamper-resistant security modules (TRSMs). TRSMs are considered tamper-responsive or physically secure devices (i.e., penetration of the device will cause immediate erasure of all PINs, secret and private cryptographic keys, and all useful residues of PINs and keys contained within it). All newly deployed ATMs and POS PIN acceptance devices are compliant with the applicable PCI PIN Entry Device and Encrypting PIN Pad Security Requirements.	□	□	□	□	□	□	
2a.	All cardholder PINs processed online are encrypted and decrypted using an approved cryptographic technique that provides a level of security compliant with international and industry standards. Any cryptographic technique implemented meets or exceeds the cryptographic strength of TDEA using double-length keys.	□	□	□	□	□	□	
2b.	All cardholder PINs processed offline using IC card technology must be protected in accordance with the requirements in Book 2 of the EMV IC Card Specifications for Payment Systems and ISO 9564.	□	□	□	□	□	□	

Objective		In Place		Cause of breach?		Contribute to breach?		Forensic Findings
		Yes	No	Yes	No	Yes	No	
3.	For online interchange transactions, PINs are only encrypted using ISO 9564–1 PIN block formats 0, 1, or 3. Format 2 must be used for PINs that are submitted from the IC card reader to the IC card.	□	□	□	□	□	□	
4.	PINs are not stored except as part of a store-and-forward transaction, and only for the minimum time necessary. If a transaction is logged, the encrypted PIN block must be masked or deleted from the record before it is logged.	□	□	□	□	□	□	
Objective 2:	*Cryptographic **keys** used for PIN encryption/decryption and related key management are created using processes to ensure that it is not possible to predict any key or determine that certain keys are more probable than other keys.*							
5.	All keys and key components are generated using an approved random or pseudo-random process.	□	□	□	□	□	□	
6.	Compromise of the key-generation process is not possible without collusion between at least two trusted individuals.	□	□	□	□	□	□	
7.	Documented procedures exist and are demonstrably in use for all key-generation processing.	□	□	□	□	□	□	
Objective 3:	*Keys are conveyed or transmitted in a secure manner.*							
8.	Secret or private keys are transferred by: a) Physically forwarding the key as at least two separate key shares or full-length components (hard copy, smart card, TRSM) using different communication channels, **or** b) Transmitting the key in cipher text form ***Note:*** *Public keys must be conveyed in a manner that protects their integrity and authenticity.*	□	□	□	□	□	□	

Objective		In Place		Cause of breach?		Contribute to breach?		Forensic Findings
		Yes	No	Yes	No	Yes	No	
9.	Any single unencrypted key component is at all times during its transmission, conveyance, or movement between any two organizational entities: a) Under the continuous supervision of a person with authorized access to this component, **or** b) Locked in a security container (including tamper-evident packaging) in such a way that it can be obtained only by a person with authorized access to it, **or** c) In a physically secure TRSM.	□	□	□	□	□	□	
10.	All key-encryption keys used to transmit or convey other cryptographic keys are (at least) as strong as any key transmitted or conveyed.	□	□	□	□	□	□	
11.	Documented procedures exist and are demonstrably in use for all key transmission and conveyance processing.	□	□	□	□	□	□	
Objective 4: *Key loading to hosts and PIN entry devices is handled in a secure manner.*								
12.	Unencrypted keys are entered into host hardware security modules (HSMs) and PIN entry devices (PEDs) using the principles of dual control and split knowledge.	□	□	□	□	□	□	
13.	The mechanisms used to load keys (such as terminals, external PIN pads, key guns, or similar devices and methods) are protected to prevent any type of monitoring that could result in the unauthorized disclosure of any component.	□	□	□	□	□	□	
14.	All hardware and passwords used for key loading are managed under dual control.	□	□	□	□	□	□	
15.	The loading of keys or key components must incorporate a validation mechanism such that the authenticity of the keys is ensured and it can be ascertained that they have not been tampered with, substituted, or compromised.	□	□	□	□	□	□	

Objective		In Place		Cause of breach?		Contribute to breach?		Forensic Findings
		Yes	No	Yes	No	Yes	No	
16.	Documented procedures exist and are demonstrably in use (including audit trails) for all key-loading activities.	□	□	□	□	□	□	
Objective 5:	*Keys are used in a manner that prevents or detects their unauthorized usage.*							
17.	Unique secret cryptographic keys must be in use for each identifiable link between host computer systems.	□	□	□	□	□	□	
18.	Procedures exist to prevent or detect the unauthorized substitution (i.e., unauthorized key replacement and key misuse) of one key for another or the operation of any cryptographic device without legitimate keys.	□	□	□	□	□	□	
19.	Cryptographic keys are only used for their sole intended purpose and are never shared between production and test systems.	□	□	□	□	□	□	
20.	All secret and private cryptographic keys ever present and used for any function (e.g., key encipherment or PIN encipherment) by a transaction-originating terminal (i.e., PED) that processes PINs must be unique (except by chance) to that device.	□	□	□	□	□	□	
Objective 6:	*Keys are administered in a secure manner.*							
21.	Keys used for enciphering PIN encryption keys (or for PIN encryption) must never exist outside of TRSMs, except when encrypted or securely stored and managed using the principles of dual control and split knowledge.	□	□	□	□	□	□	
22.	Procedures exist and are demonstrably in use to replace any known or suspected compromised key and its subsidiary keys (those keys enciphered with the compromised key) to a value not feasibly related to the original key.	□	□	□	□	□	□	

Objective		In Place		Cause of breach?		Contribute to breach?		Forensic Findings
		Yes	No	Yes	No	Yes	No	
23.	Key variants are only used in devices that possess the original key. Key variants are not used at different levels of the key hierarchy (e.g., a variant of a key-encipherment key used for key exchange cannot be used as a working key or as a master file key for local storage).	□	□	□	□	□	□	
24.	Secret and private keys and key components that are no longer used or have been replaced are securely destroyed.	□	□	□	□	□	□	
25.	Access to secret and private cryptographic keys and key materials must be limited to a need-to-know basis so that the fewest number of key custodians are necessary to enable their effective use.	□	□	□	□	□	□	
26.	Logs are kept for any time that keys, key components, or related materials are removed from storage or loaded to a TRSM.	□	□	□	□	□	□	
27.	Backups of secret and private keys must exist only for the purpose of reinstating keys that are accidentally destroyed or are otherwise inaccessible. The backups must exist only in one of the allowed storage forms for that key.	□	□	□	□	□	□	
28.	Documented procedures exist and are demonstrably in use for all key administration operations.	□	□	□	□	□	□	
Objective 7:	*Equipment used to process PINs and keys is managed in a secure manner.*							
29.	PIN-processing equipment (PEDs and HSMs) is placed into service only if there is assurance that the equipment has not been substituted or made subject to unauthorized modifications or tampering prior to the loading of cryptographic keys.	□	□	□	□	□	□	
30.	Procedures exist that ensure the destruction of all cryptographic keys and any PINs or other PIN-related information within any cryptographic devices removed from service.	□	□	□	□	□	□	

Objective		In Place		Cause of breach?		Contribute to breach?		Forensic Findings
		Yes	No	Yes	No	Yes	No	
31.	Any TRSM that is capable of encrypting a key and producing cryptograms of that key is protected against unauthorized use to encrypt known keys or known key components. This protection takes the form of either or both of the following: a) Dual-access controls are required to enable the key-encryption function. b) Physical protection of the equipment (e.g., locked access to it) under dual control.	□	□	□	□	□	□	
32.	Documented procedures exist and are demonstrably in use to ensure the security and integrity of PIN-processing equipment (e.g., PEDs and HSMs) placed into service, initialized, deployed, used, and decommissioned.	□	□	□	□	□	□	

PFI Attestation of Independence

Signatory confirms that the independence requirements described in Section 2.3 of the *QSA Validation Requirements, Supplement for PFIs* were met during this investigation.

Signature of PFI ↑	*Date:*
PFI Name:	*PFI Company:*