



Payment Application Data Security Standard (PA DSS)



Payment Application Data Security Standard (PA-DSS) October 2008

Overview

PA-DSS is the Council-managed program formerly under the supervision of the Visa Inc. program known as the Payment Application Best Practices (PABP). The goal of PA-DSS is to help software vendors and others develop secure payment applications that do not store prohibited data, such as full magnetic stripe, CVV2 or PIN data, and ensure their payment applications support compliance with the PCI DSS. Payment applications that are sold, distributed or licensed to third parties are subject to the PA-DSS requirements. (Source: PCI SSC)

In response, VeriFone has begun submitting new US applications to the proper auditing firms to ensure compliance with the security mandate.

Definitions

- "PCI SSC" refers to the PCI Security Standards Council, LLC.
- "PABP" will mean Visa's former Payment Application Best Practices program, upon which the Payment Application Data Security Standard ("PA-DSS") was based.
- "PA-DSS" is the Payment Application Data Security Standard program as established by the PCI SSC.
- "Payment Applications" refer broadly to all payment applications that store, process, or transmit cardholder data as part of authorization or settlement, where these payment applications are sold, distributed, or licensed to third parties.

Applicability

The PCI PA-DSS applies to any payment application which stores, processes, or transmits cardholder data as part of authorization or settlement, unless the application would fall under the merchant's PCI DSS validation. See the PCI PA-DSS Program Guide to determine if PCI PA-DSS validation is required for any other payment applications used at the merchant location. It is important to note that PA-DSS validated payment applications alone do not guarantee PCI DSS compliance. The validated payment application must be implemented in a PCI DSS compliant environment.

Is this mandatory?

In compliance with the mandate set forth by the card associations, VeriFone has taken the proper steps to ensure that all new releases of payment applications comply with the PA-DSS security standard.

Where do I find more information online about PA-DSS?

Payment Card Industry Security Standards Council (PCI SSC) and VISA have online references designed to cover the detail of the PABP and superseding PA-DSS standards. This information is intended for both acquirer and merchant review.

Please visit the following URLs for more information:

https://www.pcisecuritystandards.org/security_standards/pa_dss.shtml

http://usa.visa.com/merchants/risk_management/cisp_payment_applications.html

Payment Application Data Security Standard (PA DSS)



Where can I confirm the applications that have passed PA-DSS approval?

Given the current transition from PABP to PA-DSS, there is currently not an online location with a list of compliant applications. It is anticipated that a site will be available in the future similar to the one that Visa maintained for PABP:

http://usa.visa.com/download/merchants/validated_payment_applications.pdf

VeriFone will continue to keep partners informed on any future updates of the PA-DSS program.

How do I know that I am using PA-DSS approved applications?

VeriFone will provide adequate documentation and indication of which applications are PA-DSS compliant. PCI SSC web site should also be reviewed regularly for any updates.

This the first time that I have heard that POS terminal payment applications must be audited. Why?

While Visa Payment Application Best Practices (PABP) served as solid guidance for application developers, POS terminal applications were considered outside of the scope of the audit guidelines since the focus tended to center on PC-based applications. With the recent transition from Visa PABP to PA-DSS, the boundaries of the program expanded to include POS terminal applications.

Who is mandating the security review and approval of payment applications? Card Associations, Processors, VeriFone?

The PCI SSC has established the guidelines and the card associations will serve as the source of enforcement. Processors/Acquirers and terminal manufacturers are the mechanisms by which the regulations will be implemented.

VeriFone's responsibilities follow Software Vendor Guidelines per PCI DSS definition:

- Creating PA-DSS compliant payment applications that facilitate and do not prevent their customers' PCI DSS compliance (The application cannot require an implementation or configuration setting that violates a PCI DSS requirement.)
- Following PCI DSS requirements whenever the vendor stores, processes or transmits cardholder data (for example, during customer troubleshooting)
- Creating a *PA-DSS Implementation Guide*, specific to each application, according to the requirements in the *Payment Application Data Security Standard*
- Educating customers, resellers, and integrators on how to install and configure the payment applications in a PCI DSS compliant manner.
- Ensuring payment applications meet PA-DSS requirements by successfully passing a PA-DSS review.

Acquirer's responsibilities follow Reseller's Guidelines per PCI DSS definition:

- Implementing only PA-DSS compliant payment applications into a PCI DSS compliant environment (or instructing the merchant to do so)
- Configuring such payment applications (where configuration options are provided) according to the *PA-DSS Implementation Guide* provided by the vendor)
- Configuring such payment applications (or instructing the merchant to do so) in a PCI DSS compliant manner



Payment Application Data Security Standard (PA DSS)



- Servicing such payment applications (for example, troubleshooting, delivering remote updates, and providing remote support) according to the *PA-DSS Implementation Guide* and PCI DSS.

What is the impact to software certification cycle?

Every payment application must be certified moving forward including both major and minor developments. VeriFone will complete this procedure prior to submittal of applications for processor certification.

What protections does a PA-DSS application provide that today's applications do not?

Applications that have successfully completed a PA-DSS audit are certified to not retain or compromise what is considered to be secure elements of the card's track data [full magnetic stripe data, card validation codes and values (CAV2, CID, CVC2, and CVV2), PINs and PIN blocks].

Do I need to update terminals in the field?

The only method of protecting your organization from card association penalties resulting from security breaches within your merchant portfolio is to strictly adhere to all card associate security mandates. VeriFone strongly recommends updating your install base with the latest PA-DSS approved application.