WHITEPAPER

# UNDERSTANDING PCI PA-DSS: **SECURITY FOR APPLICATIONS AND FOR ORGANIZATIONS**

The Payment Application Data Security Standard (PA-DSS) has been an instrumental part of the PCI family of standards from nearly the beginning of the PCI SSC.

It helps merchants and service providers select applications developed by other parties that will aid in their compliance with PCI DSS, and allows those application vendors to market their applications as capable of meeting the necessary security requirements. That said, an application's PA-DSS compliance will not address all of the user organization's security or compliance needs, and PA-DSS applies to a certain set of payment applications only and not all applications in general. In this paper, we will consider the scope and purpose of PA-DSS, discuss the elements of a PCI PA-DSS validation, and address the ways which merchants or service providers can use an application validated for PA-DSS compliance.

## PA-DSS Standard

The PA-DSS standard applies to payment applications, specifically those involved in authorization or settlement of a payment card transaction. These applications are those that a third party develops and then licenses or distributes the application to an organization that operates it in their own environment. PA-DSS is the successor standard to the Visa Payment Application Best Practices (PABP) program, which arose from the need to test applications for potential security problems that impeded compliance with the card brand standards that came before PCI DSS, such as storage of prohibited data, lack of encryption, the inability to operate on fully patched systems, or the absence of strong user authentication controls.

## PA-DSS Eligibility

PA-DSS applies specifically to payment applications, which can include, for example, point-of-sale (POS) applications that directly interface with the consumer's card, payment middleware applications that connect front-end systems with payment processors, e-commerce applications that the e-commerce merchant operates on their own web servers, or payment switch applications used by payment processing entities. It does not include applications hosted or operated by the application developer, such as software-as-a-service (SaaS) applications, applications that underlie, but don't directly handle payment transactions, such as database or operating system software (although these might act as essential components of a valid payment application), or applications that don't handle authorization or settlement.

## PA-DSS Validation

A PA-DSS validation applies to the specific version of the application assessed: just because version 1.0 of the application demonstrated compliance with PA-DSS doesn't mean that 2.0 has, and thus a new release of the software often merits a new PA-DSS assessment. The advent of versions 3.0 and 3.1 of PA-DSS allow for some additional elements of flexibility when the application developer makes a change to the application, however, navigating these has some complexity beyond the scope of this paper. Because an application's security depends so significantly on its installation and use, PA-DSS requires that the application developer produce what's called a PA-DSS Implementation Guide, which is a detailed, specific series of instructions to correctly install, configure, operate, and maintain the application in such a way that it helps meet the PCI DSS requirements affected by the application.

An assessment involves a QSA with a specific payment application credential, a PA-QSA. PA-QSAs perform PA-DSS application testing on the application under review, usually in their own testing labs, although some times at the lab facilities of their clients. A PA-QSA tests the application in an environment that meets PCI DSS compliance and following the instructions provided by the PA-DSS Implementation Guide. The PA-QSA has to perform test transactions with the application and operate it in a way that simulates actual use of the application's features and security mechanisms. Additionally, the PA-QSA performs forensic testing on the application to determine how it handles transaction data, including sensitive authentication data (SAD), such as magnetic stripe or card security code data. Testing also includes the application's ability to meet other requirements such as providing secure authentication features, not forcing the use of default user accounts, logging appropriate activity, and facilitating secure remote access and software updates. The assessor also examines the software developer's secure software development process and reviews the PA-DSS Implementation Guide for completeness and accuracy.

Once the review and the report is complete, the PA-QSA submits a Report on Validation (ROV), Attestation of Validation (AOV), and the PA-DSS Implementation Guide to the PCI SSC for review. The PCI SSC invoices the software developer for review and listing of the application and the SSC's Assessor Quality Management (AQM) team reviews the ROV with the PA-QSA before approval and listing on the PCI SSC's list of Validated Payment Applications. Listings for a particular version of the application require an annual re-validation process, which, depending on changes to that version, may require full or partial re-assessment. Each listing has an expiry date that corresponds to the expiration of the version of PA-DSS under which the application was validated, and applications reaching their expiry must undergo full re-assessment under the at-the-time current version of PA-DSS.

Merchants or service providers looking to select a validated payment application should consider a few key elements. They should check the version of the application they wish to run against the PA-DSS list as well as the tested operating systems and platforms. This information on the listing shows which underlying components, such as operating systems and databases, the PA-QSA used to test the application, and an application is only said to be operating in a manner consistent with PA-DSS when using a set of tested platforms. So even if the application developer supports other operating systems, web servers, or similar platform components, if the testing did not include those components, running an application using those untested platforms or components may jeopardize the security of the application. Lastly, the organization should confirm that they have the correct version of the PA-DSS Implementation Guide (that corresponds specifically to the version of the application), and that they follow its instructions for installation, configuration, and maintenance.

While PA-DSS does not supplant the need for PCI DSS compliance, it can provide significant assistance for organizations that make use of validated payment applications. Provided that those organizations use the application properly, they can have some assurance that their chosen payment application will facilitate and not preclude their own PCI DSS compliance efforts.

**JACOB ANSARI**
Schellman
Manager

Jacob Ansari is a Manager at Schellman & Company, Inc.  Jacob performs and manages PCI DSS assessments. Additionally, Jacob oversees other Payment Card Industry assessment services, namely PA-DSS and P2PE. Jacob's career spans fifteen years of information security consulting and assessment services, including network and application security assessments, penetration testing, forensic examinations, security code review, and information security expertise in support of legal matters. Jacob has performed payment card security compliance assessments since the payment card brands operated their own standards prior to the advent of PCI DSS. Jacob speaks regularly to a variety of audiences on matters of information security, incident response, and payment card compliance strategy.