Visa Business News

Data Security

6 May 2021

Updates to the PCI Software Security Framework Published

Global | *Acquirers, Issuers, Processors, Agents*

Visa, Interlink, Plus Networks; V PAY; Europe Processing

Overview: Updates to the Payment Card Industry (PCI) Software Security Framework will support the validation of payment software intended for use on hardware terminals, as well as expand the eligibility scope to include all vendors of software that may be present in payment environments and vendors of any software that stores, processes or transmits payment data.

The PCI Software Security Framework (SSF) standardizes and consolidates software security principles and practices for payment software and software development entities under a single requirements architecture. The two standards within the SSF are the PCI Secure Software Lifecycle (Secure SLC) Standard and the PCI Secure Software Standard, each with a supporting program to manage validations and listings. The PCI Secure Software Standard expands on the key principles of protecting payment applications and data, which were first introduced in the Payment Application Data Security Standard (PA-DSS), and is designed to support an expanded program eligibility for payment software that is not eligible for validation under PA-DSS.

Key Updates

While there are no new requirements added to the Secure SLC Standard, this release consists of minor updates to address errata, improve readability and clarify intent. Further, all references to "payment software" have been replaced with "software" due to eligibility scope expansion in the Secure SLC program.

The revised eligibility will include all vendors of software that may be present in payment environments and vendors of any software that stores, processes or transmits payment data. Eligible software vendors will be able to demonstrate to their customers, business partners, and other key stakeholders that they have implemented and maintained appropriate practices to ensure the security of their software products throughout the software lifecycle.

As a result of a new Terminal Software Module in the Secure Software Standard, payment software intended for use on hardware terminals becomes eligible for validation under the Secure Software Program. The module defines requirements for software intended for deployment and execution on payment terminals that are PCI-approved Point-of-Interaction (POI) devices.[1] Payment software on non-validated POI devices will also be eligible for validation and listing when validated to the Core and Account Data Protection modules. The revision also addresses errata, provides minor updates and clarification.

Transition Software from PA-DSS to the PCI SSF

Payment application vendors with currently validated PA-DSS applications are encouraged to transition to the SSF. Submission of new payment applications for PA-DSS validation will be accepted until **30 June 2021**. Existing PA-

DSS validated applications will remain on the "List of Validated Payment Applications" and vendors can continue to submit changes as they normally would until the PA-DSS program closes on **28 October 2022**. When the PA-DSS program officially closes, all PA-DSS validated application listings will be moved to the "Acceptable Only for Pre-existing Deployments" list.

[1] Point of interaction (POI) refers to an electronic-transaction-acceptance product. A POI consists of hardware and software and is hosted in acceptance equipment to enable a cardholder to perform a card transaction. Therefore, the POI may be attended or unattended. POI transactions include integrated chip, magnetic-stripe and contactless payment-card-based payment transactions.

For More Information

Merchants and third party agents should contact their acquirer.