Which Applications are Eligible for PA-DSS Validation? A Guiding Checklist

Within the payment industry, there are all sorts of "payment applications" that are available for merchants to implement within their transaction environments. As much as the PA-DSS provides industry standards for developing payment applications, not all software applications that play a role in transactions are eligible for review and listing by the PCI SSC under the PA-DSS program.

For the purposes of PA-DSS, a payment application eligible for review and listing by the PCI SSC is defined as an application that:

a) stores, processes, or transmits cardholder data as part of authorization or settlement; and

b) is sold, distributed, or licensed to third parties

The following list of questions is designed to assist in further differentiating whether or not a software application is eligible for review and listing by the PCI SSC as part of the PA-DSS program.

For more detailed information, review the PCI PA-DSS Program Guide: https://www.pcisecuritystandards.org/security_standards/pci_pa_dss.shtml.

PCI SSC Founders

If the answer is YES to ANY of the following questions, **the application is NOT eligible for validation under PA-DSS.**

1. Is this a beta version of the application?
2. Does the application handle cardholder data, but the application itself does not facilitate authorization or settlement?
3. Does the application facilitate authorization or settlement, but has no access to cardholder data or sensitive authentication data?
4. Does the application require source code customization or significant configuration by the customer (as opposed to being sold and installed "off the shelf") such that the changes impact one or more PA-DSS requirements?
5. Is the application a back-office system that stores cardholder data but does not facilitate authorization or settlement of credit card transactions? For example:
   - Reporting and CRM
   - Rewards or fraud scoring
6. Is the application developed in-house and only used by the company that developed the application?
7. Is the application developed and sold to a single customer for the sole use of that customer?
8. Does the application function as a shared library (such as a DLL) that must be implemented with another software component in order to function, but that is not bundled (that is, sold, licensed and/or distributed as a single package) with the supporting software components?

Participating Organizations

Merchants, banks, processors, developers and point-of-sale vendors

9. Does the application depend on other software in order to meet one or more PA-DSS requirements, but is not bundled (that is, sold, licensed and/or distributed as a single package) with the supporting software?
10. Is the application a single module that is not submitted as part of a suite, and that does not facilitate authorization or settlement on its own?
11. Is the application offered only as software as a service (SAAS) that is not sold, distributed, or licensed to third parties?
12. Is the application an operating system, database or platform; even one that may store, process, or transmit cardholder data?
13. Does the application operate on any consumer electronic handheld device (e.g., smart phone, tablet or PDA) that is not solely dedicated to payment acceptance for transaction processing?

Please note that the above list is intended for illustration purposes only, is not exhaustive, and may be amended at any time by PCI SSC.

What should a merchant or service provider do if they use, or wish to use, applications that store, process or transmit cardholder data that are not eligible for PA-DSS validation?

Applications that store, process or transmit cardholder data and that are not eligible for PA-DSS validation would be included as part of an entity's annual PCI DSS assessment to ensure that the application is compliant with all applicable PCI DSS requirements.

What should an application vendor do if their product is not eligible for validation under the PCI SSC's PA-DSS Program?

If an application is not eligible for validation under the PCI SSC's PA-DSS program, the PCI SSC recommends that those applications, if intended for use in the cardholder data environment, are developed using PA-DSS as a baseline for protection of payment card data.

Merchants and service providers using or wishing to use such applications in their cardholder data environment would include these applications as part of their annual PCI DSS assessment.

Please note that each payment brand manages their own compliance validation programs, which may include conditions for use of non-PA-DSS validated applications, reporting requirements, due dates, fines and penalties, etc. For information about the individual payment brands' compliance requirements, please contact your acquirer (merchant bank) or the payment brands directly.