Payment Card Industry (PCI)
Payment Application Data Security Standard

Frequently Asked Questions for Transition from PA-DSS v3.0 to v3.1

June 2015

FAQs for Transition from PA-DSS v3.0 to v3.1

Q1: When does PA-DSS v3.1 become effective?

A: *PA-DSS v3.1 is effective June 1, 2015. Application validations to PA-DSS v3.0 will be accepted until August 31st, 2015. Effective September 1, 2015, all new payment applications must be validated against PA-DSS v3.1 (with AOV v3.1).*

Applications being validated against PA-DSS v3.0 which are "in queue" (i.e., submitted to the portal with invoice paid prior to September 1, 2015) will have until November 30, 2015 to complete the validation process.

Q2: When is the expiry date for payment applications validated against PA-DSS v3.1?

A: *The expiry date for payment application listings validated to PA-DSS v3.1 is October 28, 2019. See also FAQ 1275 "What are the PA-DSS Expiry Dates?"*

Q3: Can a Low Impact change be submitted to transition a PA-DSS v3.0 application to PA-DSS v3.1?

A: *Yes, a Low Impact change may be submitted as long as the change meets the criteria defined in PA-DSS Program Guide v3.0 for a Low Impact Change, and is accompanied by AOV v3.1.*

Q4: Can a No Impact change be submitted to transition a PA-DSS v3.0 application to PA-DSS v3.1?

A: *No; per the PA-DSS Program Guide, No Impact changes are limited to changes that have no impact to PA-DSS Requirements or Payment Application security, PA-DSS related functions, tested platforms, operating systems or dependencies.*

Q5: Can a delta assessment be submitted to transition a PA-DSS v3.0 application to PA-DSS v3.1?

A: *Yes, as long as the change meets PA-DSS Program Guide v3.0 criteria for a delta assessment, and is accompanied by AOV v3.1.*

Q6: How is the annual revalidation process for PA-DSS validations affected?

A: *AOV v3.1 will include an additional checkbox requiring the software vendor to confirm that the application only uses or supports the use of cryptographic protocols that meet PCI SSC's definition of strong cryptography. AOV v3.1 may be used immediately upon publication, and must be used for annual revalidations after November 30, 2015. If the vendor cannot attest to this then the annual revalidation cannot be accepted and the application moves to the Acceptable only for Pre-Existing deployment listing.*

Q7: Will the PA-DSS Program Guide be updated as well?

A: *Yes, from time-to-time, PCI SSC updates the Program Guide and as such a planned publication is forthcoming for general clarifications. However, this is not linked to the standard itself and validations against PA-DSS v3.1 may be completed using the current PA-DSS Program Guide v3.0.*

Q8: Why must new validations use PA-DSS v3.1 after August 31, 2015 when SSL and early TLS can be used as security controls within PCI DSS until June 30, 2016?

A: *In order to ensure effective security and minimize risk to cardholder data environments, payment applications must support PCI DSS compliance; since payment applications may be deployed and installed in many cardholder data environments, they have potential for significantly greater impact if not fully compliant with PA-DSS and supportive of PCI DSS compliance.*