Payment Card Industry (PCI)
Payment Application Data Security Standard

Frequently Asked Questions for Transition from PA-DSS v3.1 to v3.2

June 2016

FAQs for Transition from PA-DSS v3.1 to v3.2

Q1: When does PA-DSS v3.2 become effective?

A: *PA-DSS v3.2 is effective 1 June 2016. Application validations to PA-DSS v3.1 will be accepted until 31 August, 2016. Effective 1 September 2016, all new payment applications must be validated against PA-DSS v3.2 (with AOV v3.2).*

New payment applications validated against PA-DSS v3.1 which are "in queue" (i.e., submitted to the portal and invoice paid prior to 1 September 2016) will have until 1 December 2016 to complete the validation process.

Q2: When is the expiry date for payment applications validated against PA-DSS v3.2?

A: *The expiry date for PA-DSS v3.2 validated payment applications is 28 October 2022. 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 or v3.1 application to PA-DSS v3.2?

A: *Yes, a Low Impact change may be submitted as long as the change meets the criteria defined in PA-DSS Program Guide v3.2 for a Low Impact Change, and is accompanied by AOV v3.2.*

Q4: Can a No Impact change be submitted to transition a PA-DSS v3.0 or v3.1 application to PA-DSS v3.2?

A: *No, Administrative and No Impact changes cannot be used to transition between versions of PA-DSS. (Please see section 5.3 of the PA-DSS Program Guide).*

Q5: Can a delta assessment be submitted to transition a PA-DSS v3.0 or v3.1 application to PA-DSS v3.2?

A: *Yes, as long as the change meets PA-DSS Program Guide v3.2 criteria for a delta assessment, and is accompanied by AOV v3.2.*

Q6: Can a High Impact, Low Impact, or No Impact Change (per PA-DSS Program Guide v2.0) be submitted to transition a PA-DSS v2.0 application to PA-DSS v3.x?

A: *No, PA-DSS v2.0 payment applications will need to undergo a full PA-DSS v3.x assessment by a PA-QSA in order for it to be considered for PA-DSS v3.x validation.*

Q7: How is the annual revalidation process for PA-DSS validations affected?

A: *Similar to AOV v3.1, AOV v3.2 includes a 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 v3.2 may be used immediately upon publication, and must be used for annual revalidations beginning 1 September 2016. 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 Deployments *listing.*

Q8: 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.*

Q9: Why must new validations use PA-DSS v3.2 after August 31, 2016 when SSL and early TLS can still be used as security controls within PCI DSS until 30 June 2018?

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.*