Payment Card Industry Payment Application Data Security Standard (PCI PA-DSS)

Developing Secure Payment Applications

If you are a payment software developer or integrator of commercialized payment applications which will be used in an environment that is subject to PCI DSS compliance, you should consider assessing your payment application against the PCI Payment Application Data Security Standard (PCI PA-DSS). This standard was created to help software vendors develop secure payment applications to be sold, distributed or licensed to third parties.

Merchants are motivated to use PA-DSS validated payment applications in their payment environment to help with their PCI DSS compliance obligation and reduce cybersecurity risk.

PCI Software Security Standard is coming...

PCI recently published the two requirements documents for PCI Software Security, which will eventually replace PA DSS. These two documents are the Software Development Lifecycle (SDLC) audit requirements and Software Security Standard testing requirements. The audit requirements allow for companies to pre-validate their security development processes, to reduce the burden of on-going compliance, and the testing requirements allow for the direct assessment of the security posture of a particular software component or product.

How will these standards be applied, what do they mean to your business, and how can you best prepare for the eventual replacement of PA DSS? Talk to UL today to find out!

Advisory Services

- PCI PA-DSS Compliance Support
- PCI PA-DSS Strategy and Implementation
- PCI PA-DSS Training

Assessment Services

- PCI PA-DSS Gap Assessment
- PCI PA-DSS Formal QSA Assessment

Are you complying to all that you need?

Depending on your role in the payment ecosystem, you may need to comply to more than one PCI program. As the sole security industry expert offering the most number of PCI services globally, UL helps you simplify all of your PCI compliance needs for a cohesive risk management program.

UL is also the only Approved Application Scanning Validator (ASVV) and Consumer Electronic Clearing System Approved Evaluation Facility.

PCI Data Security Standard (PCI DSS)

All entities that store, process, or transmit cardholder data must comply to PCI DSS – including merchants, issuers and acquirers. It also applies to entities that can impact the security of the cardholder data environment like point-of-sale terminal and software vendors, cloud service providers and data centers.

PCI PIN

All entities responsible for secure management, processing, and transmission of personal identification number (PIN) data during online and offline payment card transaction processing at ATMs and payment terminals must comply to the requirements stated in PCI PIN. Entities include payment processors, acquirers, terminal vendors and key injection facilities (KIFs).

PCI PIN Transaction Security (PCI PTS)

PCI PTS focuses on the physical and logical security of devices used to protect cardholder PINs and other payment processing related activities. Financial institutions, processors, merchants and service providers are advised to only use devices that have been tested and approved under the PCI PTS program.

PCI Token Service Providers PCI TSP)

PCI TSP focuses on the physical and logical security of Token Service Providers – to protect the environments where the TSP performs tokenization services. The standard applies to all entities that generate and issue EMV payment tokens.

PCI Point to Point Encryption (PCI P2PE)

PCI P2PE is a cross-functional program incorporating various PCI security standards. It addresses both the physical and logical security of point-to-point encryption solutions. The program applies to P2PE solution vendors, P2PE component providers, P2PE application vendors, and other third-party entities like data centers who are part of a P2PE solution.

PCI 3-D Secure (3DS)

PCI 3DS Core security standard applies to entities who provide 3DS Server (3DSS), 3DS Directory Server (DS) or Access Control Server (ACS) functions as part of a 3DS solution. Entities need to discuss with the relevant card brands to determine when they need to go through a formal assessment as per the PCI 3DS Core standard.

PCI Software-based PIN Entry on COTS (PCI SPOC)

This standard addresses the physical and logical security of a payment-acceptance solution that allows a cardholder's PIN to be entered on a commercial-off-the-shelf (COTS) device. PCI SPOC applies to entities developing PIN CVM applications, or managing and deploying PIN CVM solutions.

Software Security Standard (S3) Framework

The S3 framework aims to address the logical security of payment applications that support existing and future innovations in payment and software practices. Once launched, PCI PA-DSS will be integrated within this framework, including all validated PA-DSS applications.

Speak to a UL expert to find out which other PCI security standards you may need to comply with. Visit IMS.UL.com or email us at IMSecurity@ul.com.

Empowering Trust™