Payment Card Industry Point-to-Point Encryption (PCI P2PE)

Simplifying Compliance and Increasing Data Protection

P2PE is a cross-functional program to which compliance will result in validated solutions incorporating the PCI PTS, PCI PA-DSS, PCI DSS and the PCI PIN security standards.

To limit the costs and effort associated with PCI DSS compliance and to reduce cybersecurity risk, many merchants and acquirers are looking for solutions that are approved under the PCI P2PE program. A PCI P2PE solution cryptographically protects cardholder data from the point where a merchant accepts the payment card until it reaches a secure decryption environment. Since a P2PE solution can ensure cardholder data is cryptographically protected in the merchant network, it can reduce PCI DSS scope and compliance effort of merchants significantly.

All P2PE solutions that have been assessed to meet PCI P2PE, are listed on the PCI website, making it easier for merchants to identify potential P2PE solution providers.

UL has extensive experience in contributing to PCI security standards and providing a wide spectrum of cybersecurity services within the payment ecosystem. Leverage on our knowledge and expertise to move your P2PE solution through the approval process with ease.

Advisory Services

- PCI P2PE Compliance Support
- PCI P2PE Strategy and Implementation
- PCI P2PE Training

Assessment Services

- PCI P2PE Gap Assessment (including P2PE application)
- PCI P2PE Formal QSA Assessment (including P2PE application)
- Non-Listed Encryption Solution Assessment (NESA)

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 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.

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

PCI PA-DSS addresses the logical security of payment applications. This program applies to payment software vendors and terminal vendors developing secure payment applications to be sold, distributed or licensed to third-parties.

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 us at IMS.UL.com or email us at IMSecurity@ul.com.

Empowering Trust™