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

Overview

Payment Card Industry Point-to-Point Encryption (PCI P2PE) is a cross-functional program. Compliance with PCI P2PE results in technologies that have been assessed for compliance with PCI PIN Transaction Security (PTS), the PCI Data Security Standard (DSS) and the PCI PIN Security Standard.

To limit the costs and effort associated with PCI DSS compliance and reduce cybersecurity risk, many merchants and acquirers want technologies that are approved under the PCI P2PE program. A PCI P2PE device cryptographically protects cardholder data from the time a merchant accepts the payment card until it reaches a secure decryption environment. Because a P2PE device can cryptographically protect cardholder data in the merchant network, it can help significantly reduce the scope of PCI DSS, simplifying compliance for merchants.

The PCI website lists all P2PE devices that have been assessed to meet PCI P2PE, making it easier for merchants to identify potential P2PE technology providers.

At UL Solutions, we apply our extensive experience contributing to PCI security standards and providing a wide spectrum of cybersecurity services within the payment ecosystem to helping our customers navigate the P2PE approval process with ease.

UL Solutions advisory services include:

- PCI P2PE compliance support
- PCI P2PE strategy and implementation
- PCI P2PE training

UL Solutions assessment services include:

- PCI P2PE gap assessment (including P2PE applications)
- PCI P2PE formal QSA assessment (including P2PE applications)
- Non-listed encryption solution assessment (NESA)

UL Solutions

Safety. Science. Transformation.™

CS741618_0223
051.01.0123.EN.CYB

Are you meeting all requirements for compliance?

Depending on your role in the payment ecosystem, you may need to comply with more than one PCI program. As security industry experts, we offer numerous PCI services globally. UL Solutions can help you streamline your PCI compliance efforts in a cohesive risk management program.

PCI DSS

All entities that store, process or transmit cardholder data — including merchants, issuers and acquirers — must comply with the PCI DSS. The PCI DSS also applies to entities that can impact the security of the cardholder data environment, such as 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 with the requirements stated in the PCI PIN standard. Entities include payment processors, acquirers, terminal vendors and key injection facilities (KIFs).

PCI PTS

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

PCI Token Service Provider (PCI TSP)

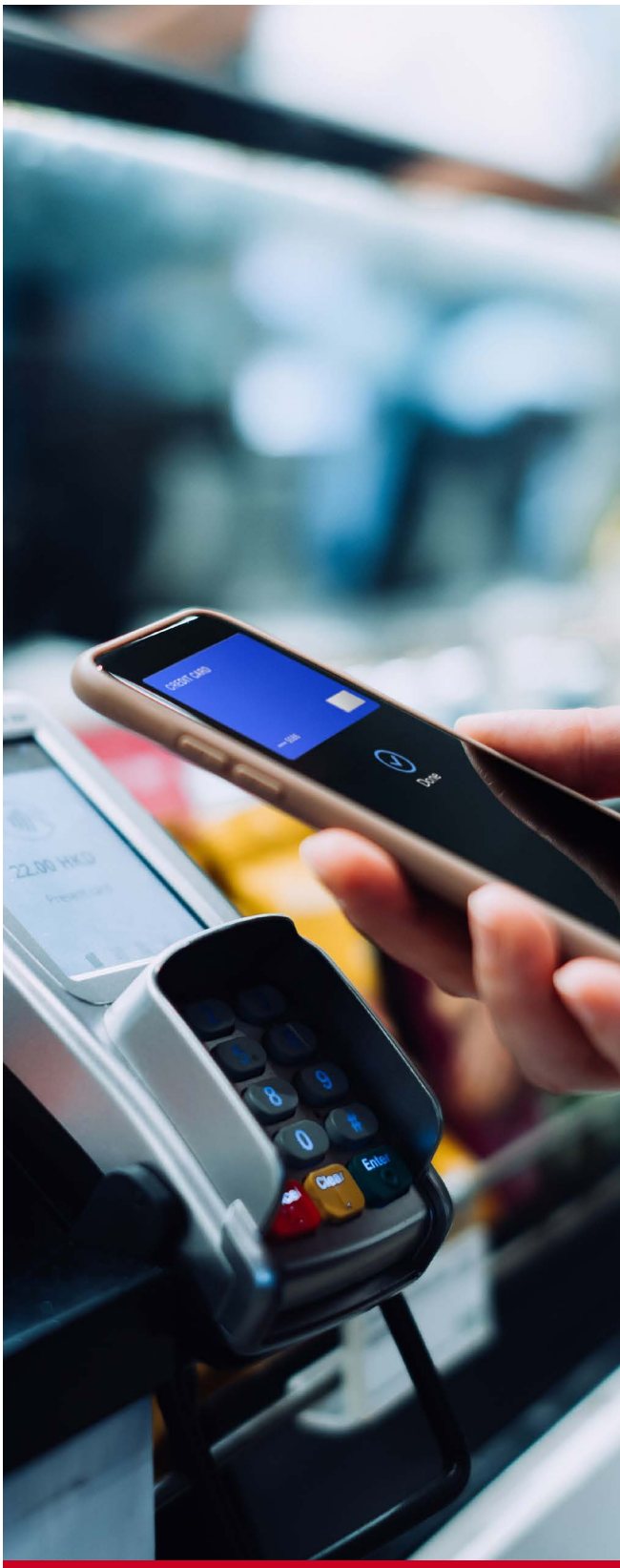
PCI TSPs focus on token service providers' physical and logical security to protect the environments where the TSP performs tokenization services. The standard applies to all entities that generate and issue EMV payment tokens.

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

This standard addresses the physical and logical security of a payment-acceptance system that allows a cardholder to enter their PIN on a commercial-off-the-shelf (COTS) device. PCI SPOC applies to entities developing PIN cardholder verification method (CVM) applications or managing and deploying PIN CVM devices.

Software Security Standard (S3) Framework

The S3 Framework addresses the logical security of payment applications that support existing and future innovations in payment and software practices.



For more information, visit UL.com/P2PE or contact one of our resellers.