Payment Card Industry Data: PIN

Secure management, processing and transmission of PIN data at ATMs and POS terminals

Throughout the processing of online and offline payment card transactions at automated teller machines (ATMs) and point-of-sale (POS) terminals, the management, processing and transmission of personal identification number (PIN) data must meet the security requirements as specified in the Payment Card Industry (PCI) PIN security standard.

The key injection facilities (KIFs) that load cryptographic keys into the POS and ATM terminals, the certification authorities (CA) and registration authorities (RAs) who might be needed to authenticate cryptographic keys used in remote key loading methods must also manage the cryptographic keys according to the PCI PIN security standard.

The latest PCI PIN security standard (i.e. PCI PIN V3) is the result of a collaboration between PCI SSC and the Accredited Standards Committee (ASC X9) to create one unified PIN Security Standard for payment stakeholders.

UL Solutions applies our payment industry knowledge and expertise helping customers navigate PCI PIN compliance. We offer a broad range of advisory and assessment services, including the following:

UL Solutions advisory services include:

- Visa PIN, TR-39 and PCI PIN compliance support
- Visa PIN, TR-39 and PCI PIN strategy and implementation
- Visa PIN, TR-39 and PCI PIN training

UL Solutions assessment services include:

- Visa PIN, TR-39 and PCI PIN gap assessment
- Visa PIN, TR-39 and PCI PIN formal Qualified PIN Assessor (QPA) assessment

UL Solutions

Safety. Science. Transformation.™

CS741600_0223
052.01.0123.EN.CYB

Do you meet the requirements for compliance?

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

PCI Data Security Standard (PCI DSS)

All entities that store, process or transmit cardholder data must comply with PCI DSS — including merchants, issuers and acquirers. The standard also applies to entities that can impact the security of the cardholder data environment, such as POS terminal and software vendors, cloud service providers, and data centers.

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 P2PE technologies. The program applies to P2PE solution vendors, P2PE component providers, P2PE application vendors and other third-party entities, such as data centers that are part of a P2PE application.

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 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 cardholder verification method (CVM) applications or managing and deploying PIN CVM devices.

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.

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.

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