Payment Card Industry PIN (PCI PIN) Security Standard

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

Throughout the processing of online and offline payment card transactions at ATMs and POS terminals, the management, processing and transmission of personal identification number (PIN) data must meet the security requirements as specified in the 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 is a PCI SSC Qualified PIN Assessor (QPA) company. As a QPA, we can assist you with the Visa PIN, TR-39 and PCI PIN assessments of your SPoC (Software-based PIN entry on COTS) solution using the latest version of the PCI PIN security standard.

Advisory Services

- 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

Assessment Services

- Visa PIN, TR-39 and PCI PIN Gap Assessment
- Visa PIN, TR-39 and PCI PIN Formal QPA Assessment

Are you in compliance?

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

We are 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. The standard 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 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 that are part of a P2PE solution.

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

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

PCI 3-D Secure (3DS)

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

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 CVM applications or managing and deploying PIN CVM solutions.

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. 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 at UL.com.

Empowering Trust™