

Media Contacts

Mark Meissner
PCI Security Standards Council
+1-202-744-8557
press@pcisecuritystandards.org
Twitter @PCISSC

PCI SECURITY STANDARDS COUNCIL UPDATES PAYMENT DEVICE STANDARD TO SUPPORT SOFTWARE-BASED PIN ENTRY ON COTS

—PCI PIN Transaction Security Point of Interaction Standard Adds New Approval Class for Secure Card Reader-PIN in Support of PCI Software-based PIN Entry on COTS Standard—

WAKEFIELD, Mass., 9 March 2018 — Today the PCI Security Standards Council (PCI SSC) published PCI PIN Transaction Security (PTS) Point of Interaction (POI) Modular Security Requirements version 5.1. The updated device standard supports the development of [PCI Software-based PIN Entry on COTS](#) (SPoC) Solutions for merchants that enable EMV® contact and contactless transactions with PIN entry on commercial off-the-shelf (COTS) devices, such as tablets and smartphones.

A summary of PCI PTS POI Modular Security Requirements version 5.1 updates are available [here](#). Key changes include:

- A new device approval class for Secure Card Reader-PIN (SCRP), a critical component in PCI SPoC Solutions as outlined in the PCI SPoC [Security](#) and [Test Requirements](#). SCRPs will be evaluated by PTS Laboratories in accordance with PCI PTS POI Modular Security Requirements version 5.1 and if compliant, approved by PCI SSC and listed on the [PCI Approved PTS Device list](#).
- Updated PCI PTS Device Testing and Approval Program Guide with a new reporting requirement for both Hardware Security Module (HSM) and POI vendors to report their compliance with PCI requirements for firmware maintenance and modifications, including open protocols.

“The new Secure Card Reader-PIN (SCRP) approval class builds upon existing account data confidentiality requirements for Secure Card Readers and adds significant security enhancements to successfully manage PIN data security,” said PCI SSC Chief Technology Officer Troy Leach. “We now get the benefit of leveraging off-the-shelf devices with payment technology designed to keep account data encrypted and confidential throughout the transaction using industry-grade PIN key management.”

Vendors can begin using PCI PTS POI Modular Security Requirements version 5.1 now for payment device evaluations. All new POI version 5 evaluations (including deltas of existing approved version 5 devices) must now use POI version 5.1.

PCI SPoC Solution evaluations must include approved SCRPs. [More information](#) on PCI SPoC Solution evaluations will be included in the PCI SPoC Solution validation program and documentation to be published in April.

PTS POI Modular Security Requirements version 5.1 and supporting documentation including PCI PTS POI Modular Derived Test Requirements, PCI PTS POI Modular Vendor Questionnaire, PTS Device Testing and Approval Program Guide, and PTS Attestation of Validation are available in the PTS section of the Document Library on the [PCI SSC website](#).

About the PCI Security Standards Council

The [PCI Security Standards Council](#) (PCI SSC) leads a global, cross-industry effort to increase payment security by providing industry-driven, flexible and effective data security standards and programs that help businesses detect, mitigate and prevent cyberattacks and breaches. Connect with the PCI SSC on [LinkedIn](#). Join the conversation on Twitter [@PCISSC](#). Subscribe to the [PCI Perspectives Blog](#).

Note to Editor: EMV® is a registered trademark in the U.S. and other countries and an unregistered trademark elsewhere. The EMV trademark is owned by EMVCo.

###