Media Contacts

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

PCI SECURITY STANDARDS COUNCIL PUBLISHES SECURITY REQUIREMENTS FOR SOFTWARE-BASED PIN ENTRY ON COTS DEVICES
—New PCI Standard to Drive Development of Secure Software-Based PIN Entry Solutions for EMV Contact and Contactless Transactions on Smartphones and Other Commercial Off-The-Shelf Devices (COTS)—

WAKEFIELD, Mass., 24 January 2018 — Today the PCI Security Standards Council (PCI SSC) announced a new PCI Security Standard for software-based PIN entry on commercial off-the-shelf devices (COTS), such as smartphones and tablets. The PCI Software-based PIN Entry on COTS (SPoC) Standard provides requirements for developing secure solutions that enable EMV® contact and contactless transactions with PIN entry on the merchant's consumer device using a secure PIN entry application in combination with a Secure Card Reader for PIN (SCRP).

"Mobile point-of-sale (MPOS) solutions have become very popular with smaller merchants for their flexibility and efficiency. MPOS has enabled them to take orders and accept payments on a tablet or smartphone, anytime and anywhere. However, some small merchants in markets that require EMV chip-and-PIN acceptance may have found the costs of investing in hardware prohibitive," said Aite Group Senior Analyst Ron van Wezel. "With the new PIN entry standard, the PCI Council has responded to market need by specifying the security requirements for allowing PIN entry directly on the mobile touchscreen. This means that merchants can accept payments with just their mobile device and a small, cost efficient card reader connected to it along with a secure PIN entry application. The payment industry will benefit overall from the wider choice in payment acceptance, as it will drive the growth of electronic transactions."

"The PCI Council has a long history of developing standards for protecting PIN as a verification method in hardware-based solutions. Existing PCI PIN Standards require hardware-based security protection of the PIN," said PCI SSC Chief Technology Officer Troy Leach. "We are now building on this foundation with a new standard that allows for an alternative approach to secure PIN entry by isolating the PIN from other data and using a new robust set of security controls that extend beyond the physical hardware device itself. The PCI Software-based PIN Entry Standard gives solution providers and application developers a baseline of security requirements specifically for accepting EMV contact and contactless transactions using software-based PIN entry."

Key security principles included in the standard's security and test requirements are:
- Active monitoring of the service, to mitigate against potential threats to the payment environment within the phone or tablet;
- Isolation of the PIN from other account data;
- Ensuring the software security and integrity of the PIN entry application on the COTS device;
- Protection of the PIN and account data using a PCI approved Secure Card Reader-PIN (SCRP).

The Software-based PIN Entry on COTS Security Requirements are for solution providers to use in designing each part of a complete solution. These requirements are available now on the PCI SSC website.

The Software-based PIN Entry on COTS Test Requirements outline testing processes for laboratories to use in evaluating solutions against the standard. These will be published in the next month, followed by a supporting program that will list PCI validated solutions on the PCI SSC website for merchant use.

For more information on the new standard, read PCI Perspectives blog post *New PCI Software-based PIN Entry on COTS Standard.*

"This standard gives solution providers and application developers a baseline of security requirements for how to securely accept PIN-based transactions on a COTS device, as well as methods to test that security is working, even as updates to the devices and applications occur frequently. PCI validated solutions will meet a robust set of security objectives that have been tested by independent laboratories," added Leach. "More and more businesses are now accepting payments with smartphones, tablets and other COTS devices, especially within the small business community. The PCI SSC Software-based PIN Entry Solution listing will provide these merchants with a resource for selecting PIN entry solutions that have been evaluated and tested by payment security laboratories, and their customers will benefit by having the best available protection for their payment data."

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.

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.

<div align="center">###</div>