Payment Card Industry
Security Standards Council, LLC

401 Edgewater Place, Suite 600
Wakefield, MA 01880
Phone: 781 876 8855

# PTS Security Requirements Version 3.0 FAQ

**Q: What are you announcing regarding PTS on Wednesday May 12, 2010?**

A: On May 12, the PCI Security Standards Council will introduce the next version, version 3.0, of the PIN Transaction (PTS) Point of Interaction (POI) security requirements. This is the result of the planned 3 year lifecycle of the PTS program and incorporates feedback shared by hundreds of stakeholders during the PTS program's multiple feedback periods.

**Q: What are the major changes introduced in version 3.0?**

A: Version 3.0 restructures the existing security requirements, simplifying the evaluation process by combining the three separate sets of POI PIN acceptance product type evaluation requirements into one, covering attended and unattended POS PIN Entry Devices along with Encrypting PIN Pad requirements (EPP). It strengthens existing requirements to increase security, and expands the scope of the program by adding three new modules for open protocols, integration and secure reading and exchange of data.

**Q: What is SRED?**

A: SRED stands for secure reading and exchange of data. The SRED module ensures that cardholder account data is protected at the point of acceptance, which will assist in meeting the required security considerations of the wider point-to-point security process. SRED is not in itself an answer to how to deploy point-to-point encryption, but is an important first step covering encryption at the point of entry.

**Q: What does SRED mean to the terminal manufacturer? To the merchant?**

A: The SRED module gives vendors a clear set of security criteria to build and test against, and enables them to provide support for point-to- point encryption. It also provides merchants with a reference listing of products tested against SRED criteria.

**Q: What does SRED mean for the Council's evaluation of point-to-point encryption?**

A; The SRED module is not a comprehensive point-to-point encryption program, but is a critical first step in building a secure point-to-point encryption infrastructure. The SRED module introduces a secure evaluation process within the PIN Transaction security program for the protection of non-PIN cardholder data.

**Q: What is Open Protocols?**

A; The Open Protocols module incorporates what was the MasterCard PTS program into PCI, and addresses POI devices that are Internet, WIFI, or GPRS enabled to make sure they are secure.

Payment Card Industry
Security Standards Council, LLC

401 Edgewater Place, Suite 600
Wakefield, MA 01880
Phone: 781 876 8855

**Q: What does Open Protocols mean to the terminal manufacturer? To the merchant?**

A; It provides manufacturers with security criteria for incorporating Open Protocols technologies into terminals. With the Open Protocols module, merchants have assurance that their terminals using Open Protocols are secure.

**Q: What is the Integration module?**

A: A new aspect of the PTS V3.0 specification is that it permits evaluation and approval of additional individual secure components, such as smart card readers, in addition to existing components such as Encrypting PIN Pads. These secure components are designed to be integrated into a final solution, and the Integration requirements ensure that this process is conducted without affecting or impacting the overall security of the final product.

**Q: What does the Integration module mean to the terminal manufacturer? To the merchant?**

A: Terminal manufacturers can purchase PCI approved secure components from various vendors and integrate them into their final solution, which itself can be approved against the PCI PTS requirements. Merchants will have assurance that security is not degraded when components are integrated into compound devices such as kiosks and automated fuel dispensers.

**Q: Are these 3 new modules mandatory for terminal vendors to test against?**

A: Any product that incorporates separate modules, such as EPP, card readers, etc. must complete the integration requirements. Products are not required to support open protocols or the secure reading and exchange of data, however, if they do, then those modules are mandatory for evaluation and approval.

**Q: What is significant about these changes?**

A: These changes simplify the overall process of security evaluation for PIN Entry devices. In merging three sets of requirements into one, version 3.0 eliminates overlapping documentation and confusion around which processes are required for each device by providing one modular set of security requirements for all PIN acceptance terminals and a single listing of approved products.

**Q: What are some of the other changes in this version?**

A: In addition to submitting complete terminals for evaluation, the revisions facilitate the ability to evaluate non-traditional form factors for specific functions and the addition of certain OEM products, such as smartcard readers for approval.

Payment Card Industry
Security Standards Council, LLC

401 Edgewater Place, Suite 600
Wakefield, MA 01880
Phone: 781 876 8855

**Q: Which documents are affected?**

A: The following updated documents will be available on the Website on May 12:

- New PTS requirements document
- Listing of approved devices, updated with additional information and graphics to make it easier to use
- New derived test requirements (DTRs) available for vendors
- New questionnaire with updated criteria for vendors to fill out and submit to labs

A new program guide and updated FAQs are also being developed and will be available in the next couple of months.

**Q: As a merchant, how do these changes affect my purchasing decisions?**

A: With the updated detailed product listing available on our website, merchants can more easily find the device that meets their needs and ensure it meets PTS requirements. PTS requirements ensure a device helps not hinders, in a merchant's PCI DSS compliance efforts.

**Q: As a vendor, how does this impact me? Do I need to do anything differently?**

A: Vendors now have one set of requirements for testing their products against, and they can begin doing so now or by April 30, 2011 when the previous set of requirements will sunset. The version 2 EPP and POS PED and the version 1 UPT security requirements will remain available for testing and new approvals until 30 April 2011. After that date, they will only be available for deltas on existing approvals, and all new approvals of POI PIN acceptance product types must use PTS v3 for those approvals.

**Q: When does a vendor have to build to these specs by?**

A: By April 30, 2011.

**Q: Can I still use my old POS terminal?**

A: Yes. No action is needed by merchants at this point. However, if your organization is upgrading equipment, you can check that it has been tested and approved against PTS requirements by viewing the listings on the PCI SSC website.

**Q: What is the deadline for deploying SRED in my organization?**

A: The use of SRED is not mandatory. As such, there is no deadline.

Payment Card Industry
Security Standards Council, LLC

401 Edgewater Place, Suite 600
Wakefield, MA 01880
Phone: 781 876 8855

**Q: I make EPP's, what does this mean for me?**

A: With the module approach, in addition to submitting a complete terminal for review, you can also now more easily determine what requirements you need to follow for testing and evaluating your specific product. In the case of encrypting PIN pads, using the appropriate modules and requirements within those modules will still enable you to obtain PCI approval for your EPP.

**Q: Will this remove confusion from the testing process?**

A: Yes, there is now one set of documentation to be followed for POI PIN acceptance product types. With the new modular approach, you can easily determine which components you need to test and evaluate and follow the specific requirements for doing so.

**Q: What is the modular approach? How does it work?**

A: The modular approach provides one set of security evaluation requirements for all POI PIN acceptance product types. The requirements are broken out by specific modules and requirements within those modules that pertain to specific functionality. Regardless of form factor of the device or component that is under evaluation, the functionalities that it provides drive the applicability of the criteria. Functionalities may include PIN entry, key management, card reading, provides feedback to cardholders, device is a module, device is compound, implements open protocols and protects account data.

This approach not only enables manufacturers to submit entire terminals for review, but also it allows OEMs to easily determine the criteria specific to their product or component and submit it for evaluation using the requirements for the applicable module(s).

It provides merchants with a simplified view of product listings so they can easily locate the device that meets their needs and ensure it's approved.

**Q: What impact does this have on PCI DSS or PA-DSS?**

A: Previously, PTS requirements focused primarily on the protection of the cardholder's PIN when used in connection with a financial transaction. PCI DSS addresses additional sensitive data such as PAN and cardholder name and focuses on the transmission and storage of this information. With the PTS requirements version 3.0, it's now that much easier for device vendors and their customers to secure sensitive card data at the point of interaction, so that in combination with PCI DSS and PA-DSS, the processing, transmitting and storage of account data is better protected.