

Payment Card Industry POS PED and EPP Update

Jeremy King, Business Leader, Payment System Integrity

Applies To: Acquirers

Summary: As of 31 December 2007, all pre-Payment Card Industry (PCI) point-of-sale (POS) PIN entry device (PED) approvals have expired. As such, acquirers and their merchants must only deploy PCI-approved terminals and encrypting PIN pads (EPPs). Acquirers or their merchants that may be partially through a deployment must apply for a waiver to complete deployment.

Details about the deployment and migration of terminals are provided below.

Action Indicator: **M** Mandate

Effective Date: **31 December 2007**—All pre-PCI approvals expired

1 March 2008—Last date for submission of terminals for evaluation against version 1.3 of the PCI POS PED

1 March 2008—Last date for submission of EPPs for evaluation against version 1.0 of the PCI EPP

1 May 2008—From this date, MasterCard will evaluate all newly submitted products against version 2.0 of the PCI POS PED or PCI EPP Security Requirements

Overview

All pre-PCI POS PED approvals have now expired; and beginning 31 December 2007, all newly deployed, re-deployed, or refurbished POS PED and EPP devices must be PCI approved.

In addition, MasterCard will begin migrating the PCI POS PED and PCI EPP Program into the control and ownership of the PCI Security Standards Council (SSC). This migration will take place 1 February 2008.

Upon completion of this transfer, MasterCard will remove all documentation, including the list of PCI-approved products, from MasterCard OnLine®. The documentation then will be available and maintained by the PCI SSC Web site.

Starting 1 May 2008, the PCI POS PED and PCI EPP Security Evaluation Program will migrate to version 2.0. Vendors that wish to submit POS PED or EPP terminals for approval against version 1.3 of the PCI POS PED and version 1.0 of the PCI EPP must submit the product to the evaluation laboratory **no later than 1 March 2008**.

Background

This article provides an update to recent and planned changes to the PCI POS PED and PCI EPP Security Evaluation Programs, which have a significant impact on members, merchants, and vendors.

When first establishing the PCI POS PED and EPP Security Evaluation Programs, MasterCard, Visa, and JCB agreed on a common set of security requirements for the evaluation testing and approval of POS PED and EPP devices. As part of the initial establishment of the programs, MasterCard and JCB agreed to grandfather products approved under the old Visa Approval Process for the lifetime of that approval. These POS PED and EPP devices were referred to as pre-PCI products. **The approval of these pre-PCI approved products lapsed on 31 December 2007.**

In addition, when establishing the PCI POS PED and PCI EPP Security Evaluation Programs, it was agreed to review the security requirements every three years. As the first set of requirements became effective on 1 January 2005, a new updated set of requirements has been developed and submitted to the industry for review. **These new requirements will become effective 1 May 2008.**

Finally, because of increased cooperation in other areas of security testing, a formal body known as the PCI Security Standards Council (SSC) was created. Initially, the council was established to ensure a common set of requirements for data security. However, it became clear that to have two processes entitled PCI—one controlled by a separate council and the other not—was confusing to members, merchants, and vendors.

End of Pre-PCI Approval

In establishing an evaluation program for POS PED and EPP devices, Visa agreed to issue an approval for a period of three years. In transferring this to PCI, MasterCard, Visa, and JCB all agreed to have a common end to the approval date of 31 December 2007.

Impact

MasterCard Standards clearly state that only PCI-approved terminals can be deployed, re-deployed, or refurbished. Therefore, as the approval of the pre-PCI terminals has now lapsed, these terminals no longer can be considered for deployment, re-deployment, or refurbishment.

MasterCard realizes that discussions between vendors, members, and merchants relating to the deployment of terminals can take several months, and that actual deployment of large numbers of terminals also can take several months. For this reason, MasterCard will offer a variance to acquirers to allow them to complete deployments of pre-PCI product during 2008. **This variance is based on the acquirer completing all deployment during 2008.**

Terminals already deployed are not affected by this change.

Launch of PCI POS PED and PCI EPP Version 2.0

As part of a continuous improvement program for improved security, MasterCard, Visa, and JCB have carried out a full and thorough review of the PCI POS PED and PCI EPP Security Requirements.

As part of this review, a number of new requirements to improve the security of terminals were added to:

- Counter various actual or possible attack methods against terminals
- Raise the standard in relation to terminal security

Details of all changes to the security requirements can be found in the relevant documents located on MasterCard OnLine.

The new security requirements will become effective 1 May 2008. To ensure a smooth transition, any vendor that wants to submit a terminal for PCI POS PED version 1.3 evaluation, or an EPP to PCI EPP version 1.0, must submit the product to the evaluation laboratory **by 1 March 2008.**

Refer to the "Documentation" section at the end of this article for a list of relevant documents.

Any product submitted after this date will be evaluated against the latest version 2.0 requirements. This requirement is necessary to enable the evaluation laboratories time to evaluate all submitted product by 30 April 2008.

All product approved against the PCI Security Requirements will be listed on MasterCard OnLine and will clearly show if it has been approved against version 1.0 or version 2.0.

Transition to the PCI SSC

When establishing the PCI POS PED and PCI EPP Security Evaluation Programs, it was necessary to show that these programs covered a majority of the card schemes and covered both chip and magnetic stripe terminals where a personal identification number (PIN) was entered.

The card schemes also adopted the PCI name for other joint evaluation programs (for example, the *PCI Data Security Standards*). As such, the card schemes decided to establish a separate legal group—the PCI Security Standards Council (SSC)—to run the PCI Data Security Standard (DSS) program. Having now established the PCI SSC, it made sense to transfer the PCI POS PED and PCI EPP Programs into the council.

This decision has several major benefits, including that the PCI POS PED and PCI EPP Programs now will be accepted by all five major card schemes and so become a truly worldwide, World Class A standard for security.

MasterCard anticipates that the transfer to PCI SSC will be completed by February 2008. When the transfer is completed, the PCI SSC will house and control all documentation and lists of approved devices on the PCI SSC Web site:

Web site: www.pcisecuritystandards.org

MasterCard then will remove documentation currently residing on MasterCard OnLine.

Documentation

Detailed documentation explaining the PCI EPP Security Evaluation Programs, including all related documentation and a list of all approved EPPs, can be found at:

1. Navigate to **www.mastercardonline.com**.
2. Log on by entering your **User ID** and **Security Information**.
3. From the **My Products** menu, select **Member Publications**.
4. From the **Manuals by Category** menu on the left, click **Security/Risk Services**.
5. Select **PIN, Terminal, and Wireless** from the flyout menu.
6. From the submenu, select **PEDs and EPPs**.
7. Click the appropriate link for the document you want to view.

For More Information

If you have questions about this information, please contact the Customer Operations Services team, your regional Help Desk, or a regional Security and Risk Services representative.