Visa Security Bulletin

Risk Management | Data Security 6 December 2012

Encrypting PIN Pads Must Be Industry-Approved

Acquirers, Issuers, Processors, Agents

Recent reports from ATM manufacturers indicate that some encrypting PIN pads (EPPs) used with ATMs sold globally are not Payment Card Industry (PCI)-approved. Visa reminds clients that they are required to purchase and deploy only PCI-approved EPPs, which undergo rigorous testing to ensure the highest level of security for cardholder PINs.

Sponsoring acquirers that are found to be noncompliant with PCI PIN Transaction Security (PTS) requirements and Visa Operating Regulations may be subject to penalties and fines.

How to Ensure EPPs Are PCI-Approved

Clients should compare their EPP inventory with the PCI Security Standards Council (SSC) list of approved PTS devices (Figure 1) to ensure the highest level of security for their organization and the payment community. Clients that purchase and deploy EPPs that do not match **all** of the identifying criteria on the list are at significant risk for device compromise, which may lead to monetary losses and diminished cardholder confidence.

Product information that **must** match the data on the PCI SSC list of approved PTS devices includes:

- Hardware number
- Firmware number (some EPPs are shipped with multiple firmware versions, so clients must ensure that the firmware activated during installation matches the list)
- Application number
- Version
- PCI approval number
- Product type
- Expiry date

These details should be reflected in all purchase orders and contracts, and clients should ensure that vendors are required to provide them with PCI-approved EPPs. Additionally, clients must take a screen shot of the PCI SSC website at the time of purchase (Figure 2) to begin an audit trail of their EPP information and show that they purchased the EPP in compliance with Visa usage mandates. Refer to the *PCI PIN Security Requirements, Version 1*, for more information on how to validate compliance.

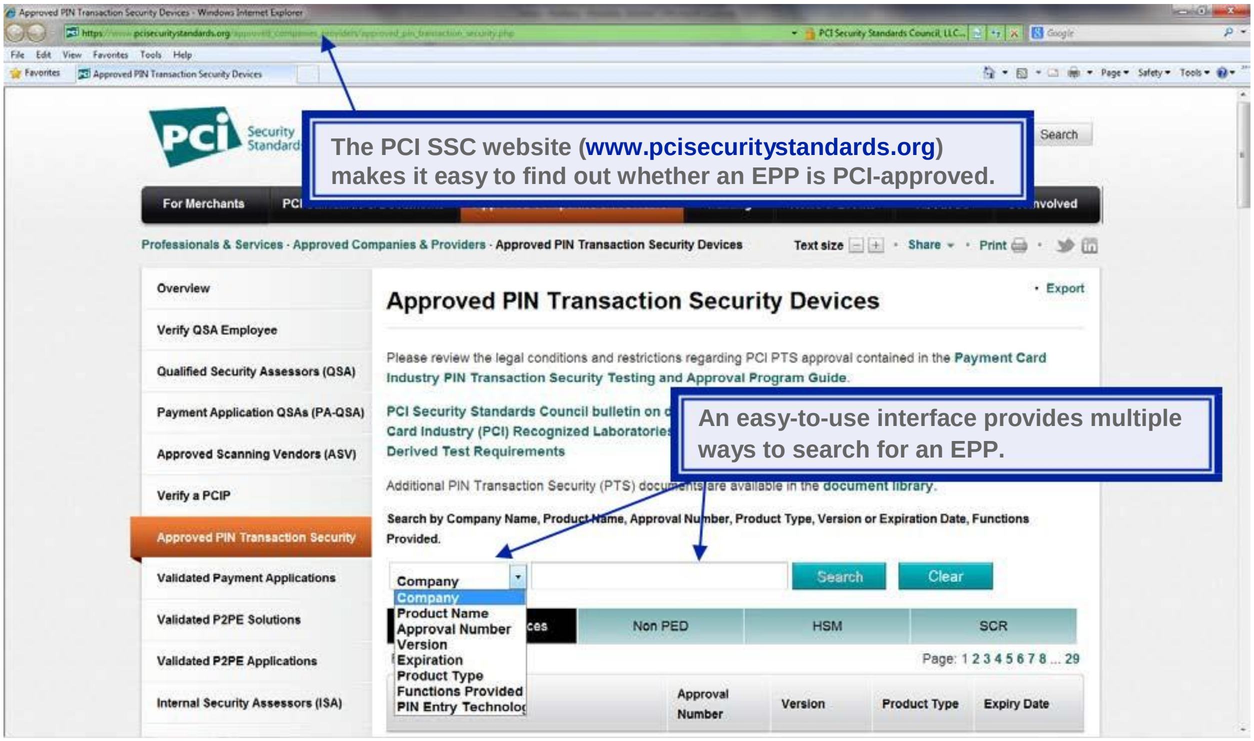
Best Practices for EPPs

Visa has not set mandatory sunset dates for any EPPs. However, vendor-attested and pre-PCI-approved EPPs should be retired first as ATMs are upgraded and replaced.

Clients also should develop ATM equipment policies that require the purchase of the latest versions of PCI- approved EPPs, as the most recent devices offer the most protection and are tested under the most rigorous standards.

PIN-processing equipment such as EPPs may be deployed only with the assurance that it has not been substituted, tampered with or modified without authorization before cryptographic keys are loaded. When the equipment is in service, precautions must be taken to minimize the threat of compromise. Refer to *General PED Frequently Asked Questions* for complete details regarding Visa rules for EPP acquisitions.

Figure 1:



The PCI SSC website (www.pcisecuritystandards.org) makes it easy to find out whether an EPP is PCI-approved.

An easy-to-use interface provides multiple ways to search for an EPP.

Approved PIN Transaction Security Devices - Windows Internet Explorer

https://www.pcisecuritystandards.org/approved_companies_providers/approved_pin_transaction_security.php

Professionals & Services · Approved Companies & Providers · Approved PIN Transaction Security Devices

Approved PIN Transaction Security Devices

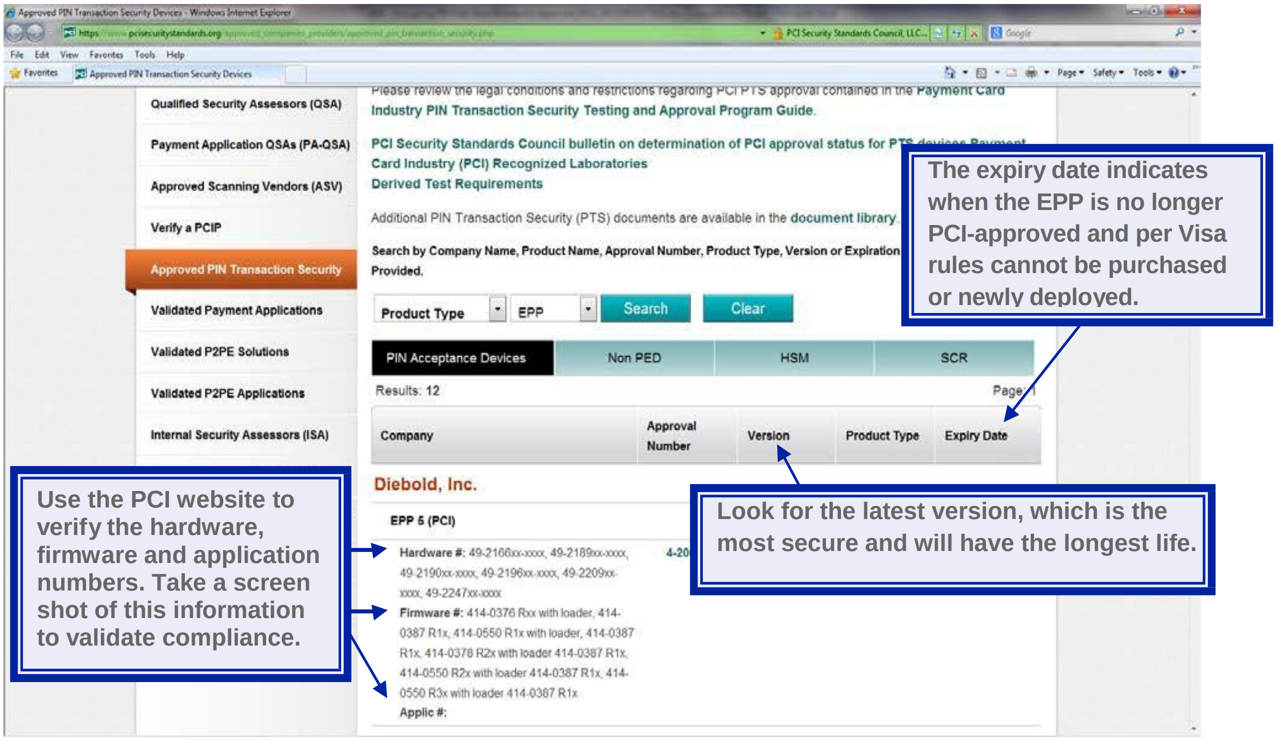
Please review the legal conditions and restrictions regarding PCI PTS approval contained in the Payment Card Industry PIN Transaction Security Testing and Approval Program Guide.

PCI Security Standards Council bulletin on c… Card Industry (PCI) Recognized Laboratorie… Derived Test Requirements

Additional PIN Transaction Security (PTS) documents are available in the document library.

Search by Company Name, Product Name, Approval Number, Product Type, Version or Expiration Date, Functions Provided.

Figure 2


Approved PIN Transaction Security Devices - Windows Internet Explorer
https://www.pcisecuritystandards.org/approved_companies_providers/approved_pin_transaction_security.php
PCI Security Standards Council, LLC...
Google
File Edit View Favorites Tools Help
Favorites
Approved PIN Transaction Security Devices
Page Safety Tools
Qualified Security Assessors (QSA)
Payment Application QSAs (PA-QSA)
Approved Scanning Vendors (ASV)
Verify a PCIP
Approved PIN Transaction Security
Validated Payment Applications
Validated P2PE Solutions
Validated P2PE Applications
Internal Security Assessors (ISA)
Search
Clear
PIN Acceptance Devices
Non PED
HSM
SCR

Please review the legal conditions and restrictions regarding PCI PTS approval contained in the Payment Card Industry PIN Transaction Security Testing and Approval Program Guide.

PCI Security Standards Council bulletin on determination of PCI approval status for PTS devices Payment
Card Industry (PCI) Recognized Laboratories
Derived Test Requirements

Additional PIN Transaction Security (PTS) documents are available in the document library.

Search by Company Name, Product Name, Approval Number, Product Type, Version or Expiration
Provided.

Product Type: EPP

Results: 12

Page: 1

Company	Approval Number	Version	Product Type	Expiry Date
Diebold, Inc.				
EPP 5 (PCI)				
Hardware #: 49-2166xx-xxxx, 49-2189xx-xxxx, 49-2190xx-xxxx, 49-2196xx-xxxx, 49-2209xx-xxxx, 49-2247xx-xxxx **Firmware #:** 414-0376 Rxx with loader, 414-0387 R1x, 414-0550 R1x with loader, 414-0387 R1x, 414-0378 R2x with loader 414-0387 R1x, 414-0550 R2x with loader 414-0387 R1x, 414-0550 R3x with loader 414-0387 R1x **Applic #:**	4-20			

The expiry date indicates when the EPP is no longer PCI-approved and per Visa rules cannot be purchased or newly deployed.

Use the PCI website to verify the hardware, firmware and application numbers. Take a screen shot of this information to validate compliance.

Look for the latest version, which is the most secure and will have the longest life.

Related Documents

Approved PIN Transaction Security Devices

General PED Frequently Asked Questions

PCI PIN Security Requirements, Version 1.0

Visa PIN Security and Key Management website

For More Information

Contact your regional Visa risk representative or e-mail pinusa@visa.com