

Encrypting PIN Pads Must Be Industry-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.

Organizations that are found to be noncompliant with Visa PIN Security Requirements may be subject to non-compliant assessments.

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

Verify these details are reflected on all purchase orders and contracts, and clients should ensure that vendors are required to provide them with PCI-approved EPPs. Additionally, as a best practice it is recommended to 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 evidence that the purchased EPP is in compliance with Visa PIN Entry Device Requirements.

Best Practices for EPPs

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:

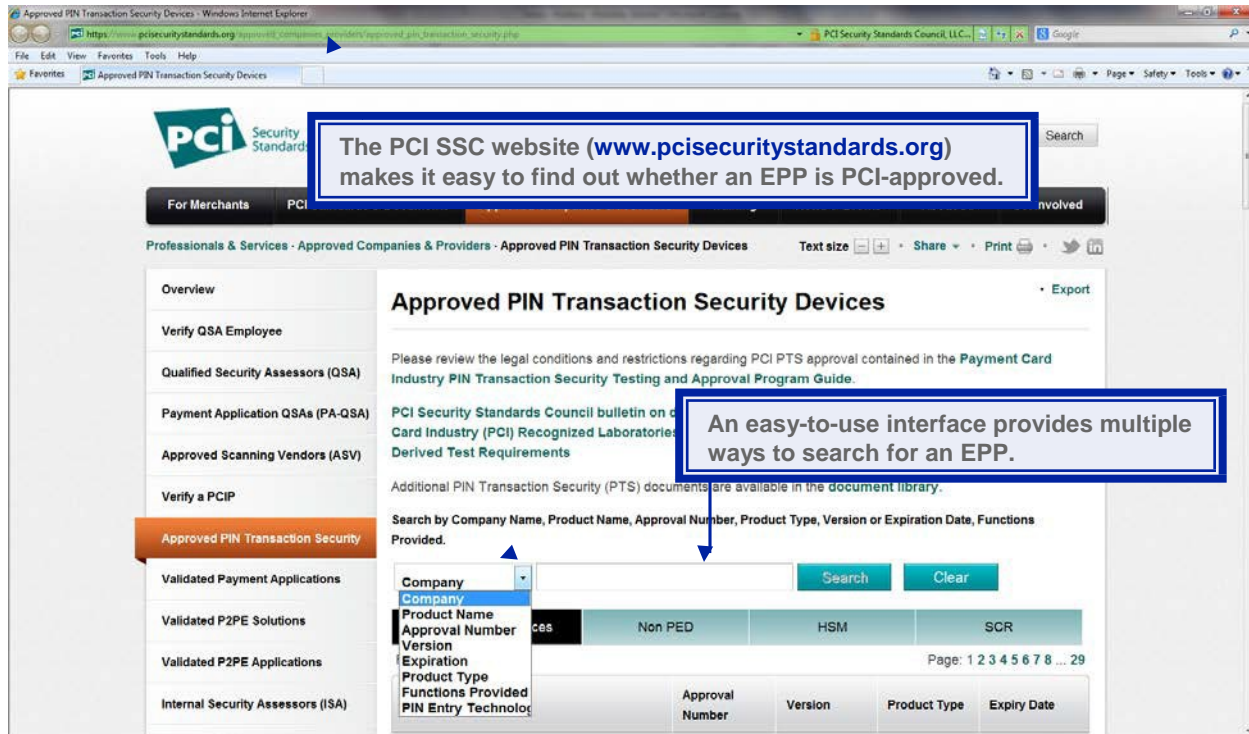
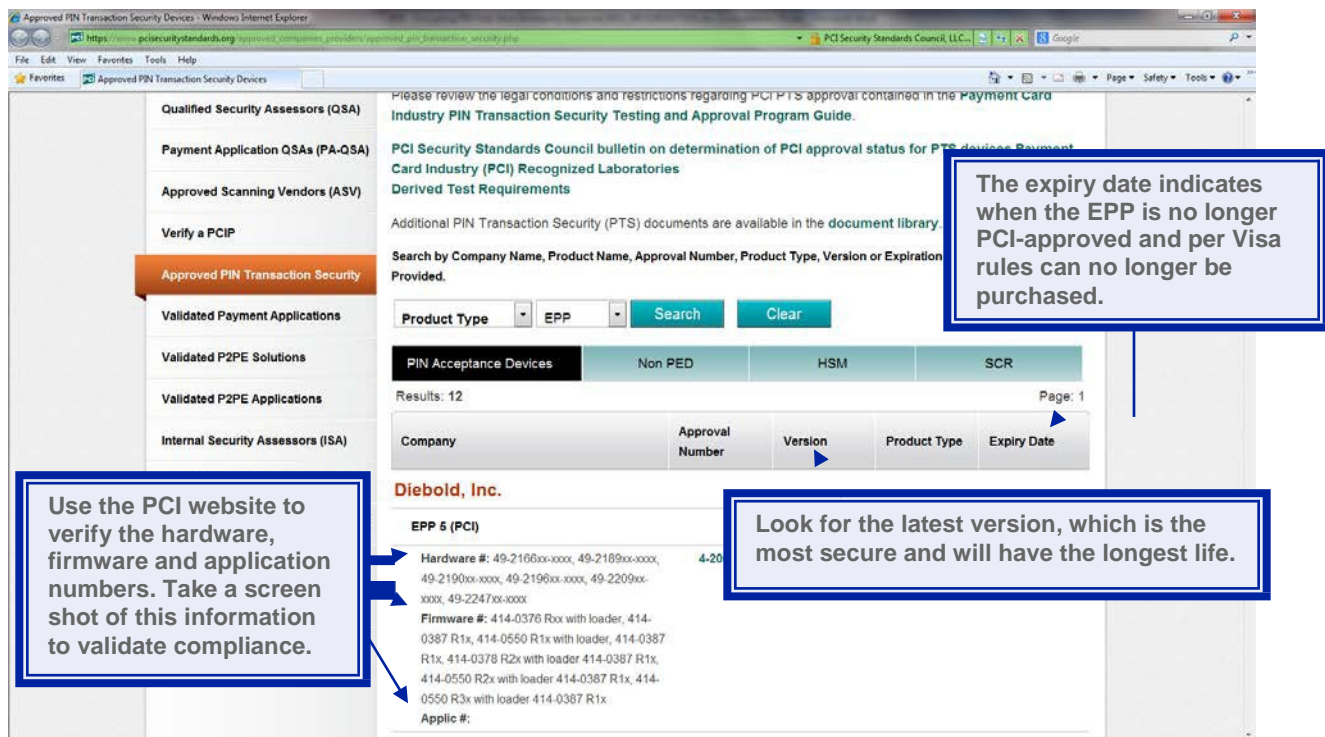


Figure 2:



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 pin@visa.com,
