Risk Management | Data Security 6 May 2013

Maximize Point-of-Sale PIN-Entry Device Security

Acquirers, Issuers, Processors, Merchants, Agents

Recently, there have been publicized reports of compromises involving pre-Payment Card Industry (PCI) attended point-of-sale (POS) PIN-entry devices (PEDs) and PCI PIN Transaction Security (PTS) Version 1.x devices.

Visa reminds clients, processors, merchants and agents that all pre-PCI attended POS PEDs must be retired by 31 December 2014. These devices are actively being targeted by criminals to skim card and PIN data, and clients should have detailed plans in place to ensure that the deadline will be met. Clients should also review Visa's Vulnerable Device Listing to ensure these devices are targeted for immediate removal due to reported compromises that have resulted in financial losses.

In addition, clients should be aware that PCI PTS Version 1.x devices are now approaching end of life, and their continued use introduces risks to the payment system. Concerns stem from the fact that these devices were tested under less robust security standards, and some have been reported as compromised or have been delisted by the PCI Security Standards Council (SSC).

All PCI PTS Version 1.x devices will expire on 30 April 2014 and cannot be purchased or newly deployed after this date. Visa recommends that clients purchase and deploy the highest version of PCI-approved PEDs using the following best practices:

- **Purchasing**
  - Clients should evaluate their current PED inventory and make plans to limit or stop purchases of PCI PTS Version 1.x devices. Your organization's policy should be to purchase the latest version of PCI-approved PEDs, which is currently PCI PTS Version 3.x and has an expiration date of April 2020.
  - Clients should check the list of Approved PIN Transaction Security Devices on the PCI website (Figure 1) to ensure that current and planned future PEDs are PCI-approved and provide the highest level of security.
  - Merchants are encouraged to upgrade their devices to support EMV acceptance (contact and contactless) in support of EMV counterfeit liability shift dates.
- **Validating Compliance**
  - Clients should ensure that the PED hardware, firmware, application and PCI approval numbers; version; product type; and expiration date (Figure 2) match the corresponding data on the list of Approved PIN Transaction Security Devices. (Refer to the *PCI PIN Security Requirements, Version 1.0*, for more information on how to validate compliance.)

    Clients must take a screen shot of PED information from the Approved PIN Transaction Security Devices list to include as part of their device records and use it as confirmation that the purchased PED is in compliance with Visa usage mandates.
  - Clients should ensure their purchase orders and contracts include language supporting the above steps, and specify to their vendors to **only** provide them with PCI-approved PEDs.
- **Deployment**
  - Clients should review the PCI PIN Security Requirements to understand their responsibility to always manage PEDs securely during their entire lifetime. This includes securing the POS PED at the cash register with locking stands or cables to prevent PEDs from being easily removed.
  - Merchants with wireless handheld POS PEDs should ensure they have inventory controls and that the devices are stored securely when not in use.
  - Clients should also establish reporting and escalation procedures for devices that have been tampered with or have gone missing.

Figure 1:

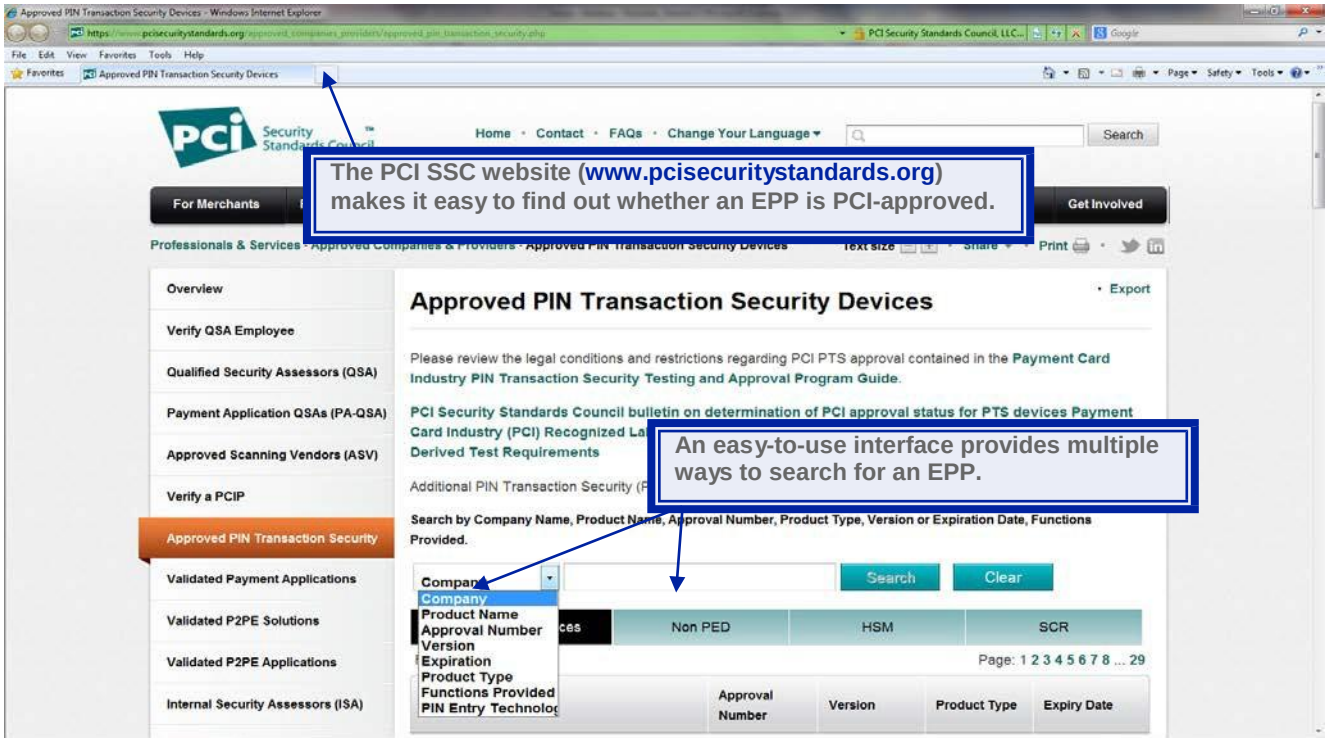
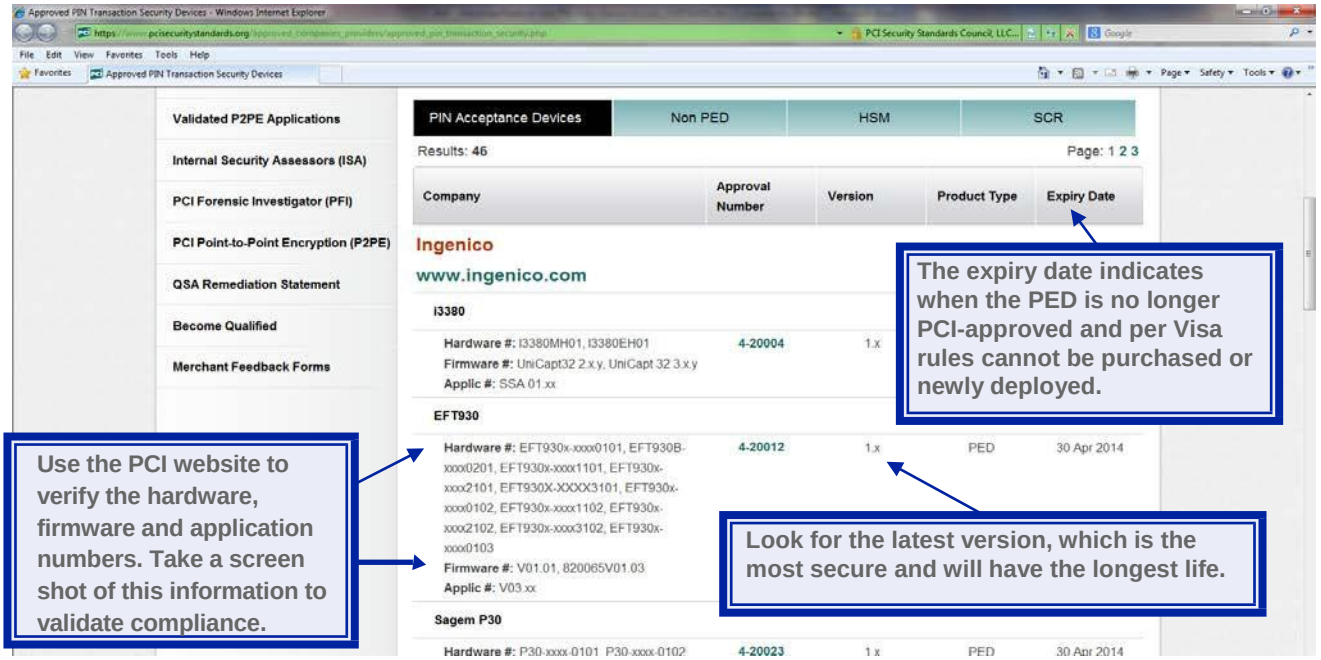


Figure 2:



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 pinna@visa.com