

VISA PIN SECURITY BULLETIN

1 May 2018

Original publication 6 December 2012

Maximize Point-of-Sale PIN-Entry Device Security

Visa reminds clients, processors, merchants and agents that all pre-PCI attended POS PEDs must be retired. 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 PIN Entry Device (PED) Requirements to understand the mandates for removal.

Clients should be aware that PCI PTS Version 1.x and 2.x devices have expired. Their continued use introduces risks to environment in which they are deployed. 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 and 2.x devices have expired and can no longer be purchased. 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 devices approaching expiration. 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*, 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 requirements.
- 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:

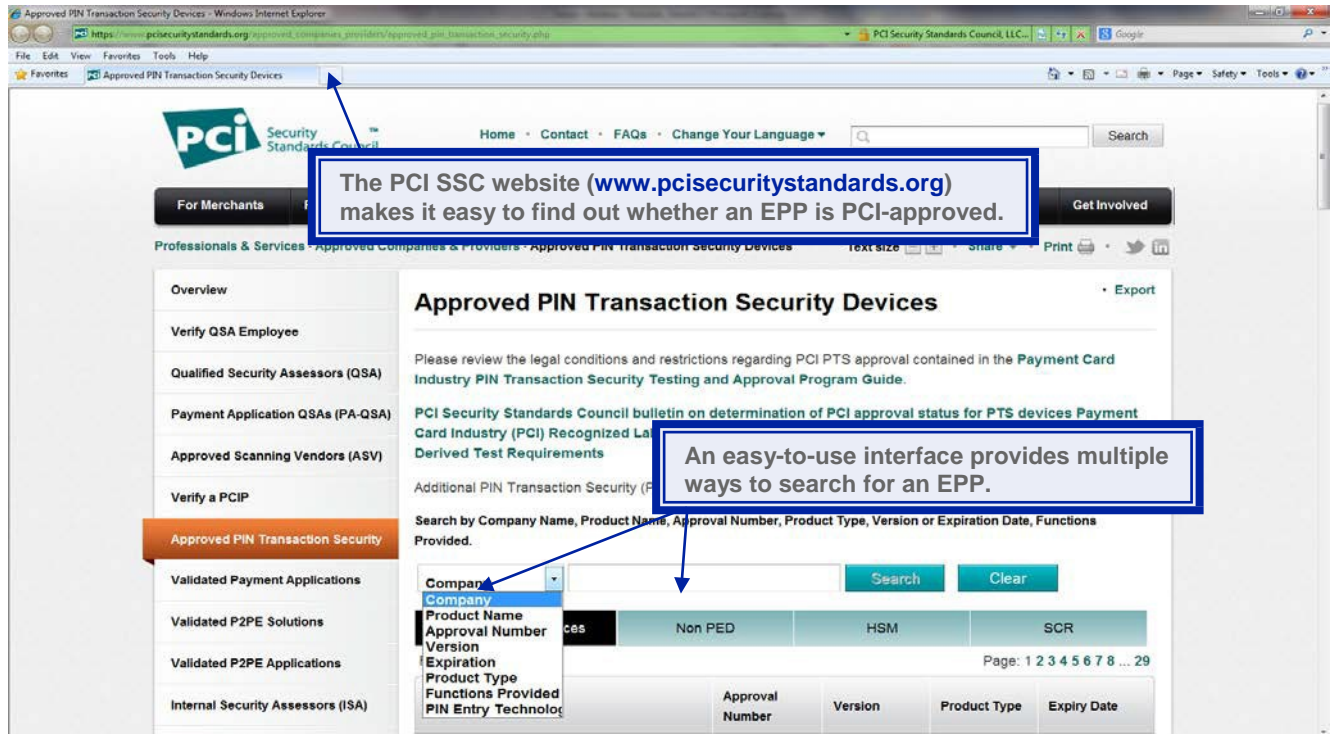
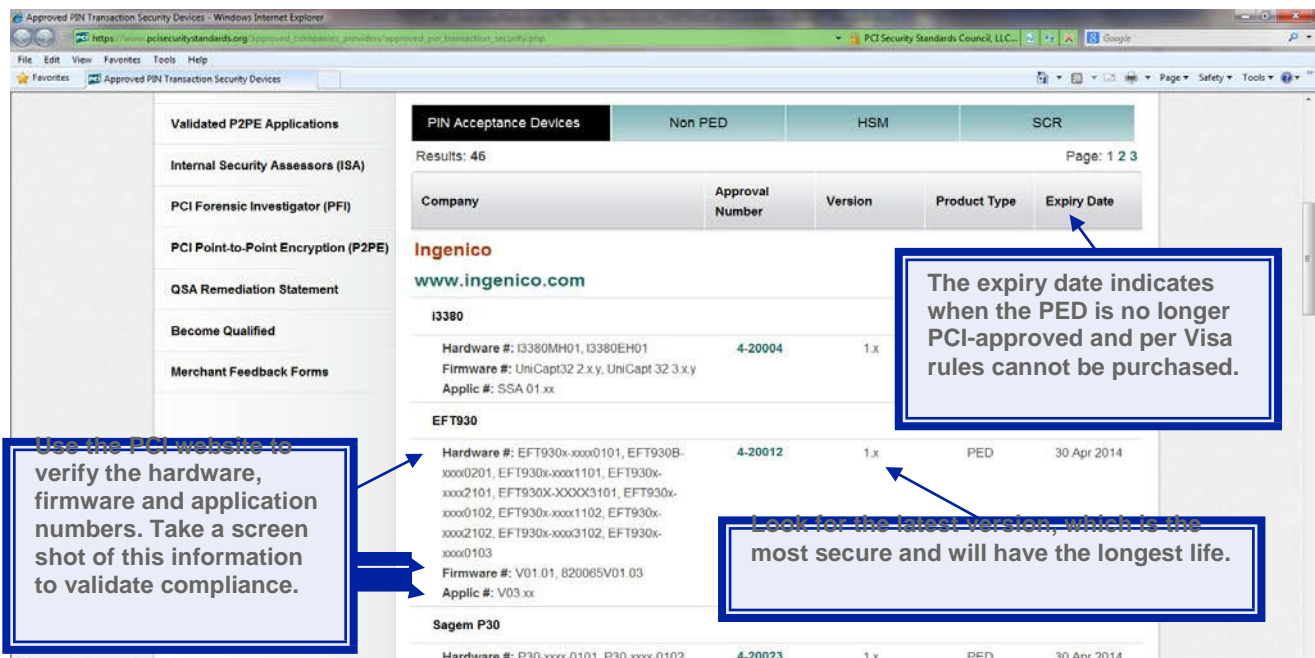


Figure 2:



Related Documents

Approved PIN Transaction Security Devices

PCI PIN Security Requirements

Visa PIN Security website

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