



PIN SECURITY BULLETIN

Interlink Merchants Must Use TDES at Point of Sale by July 2010

September 30, 2008

The confidentiality of cardholder Personal Identification Numbers (PINs) when used at point-of-sale (POS) PIN-Entry Devices (PEDs) depends on the full compliance of all payment system participants with the *Payment Card Industry (PCI) PIN Security Requirements*. To ensure the continued secure protection of PIN-based transactions, Visa established requirements for the use of Triple Data Encryption Standard (TDES) for PIN encryption at all POS PEDs. Effective July 1, 2010, all Interlink-accepting POS PEDs and host systems must use TDES for the protection of PINs.

In August 2005, Visa announced end-to-end requirements for the use of TDES to protect online and offline PIN-based transactions processed within POS and host systems. Since 2003, many payment system participants, agents, merchants and processors have deployed TDES-capable POS PEDs and have started *using* TDES with at least double-length keys to protect PINs. This requirement ensures the continued protection of these transactions. To protect all payment system participants and the Visa payment system, it is essential that acquirers and their agents, merchants and processors finalize implementation plans for the migration to TDES as quickly as possible. Visa will be contacting Interlink-sponsoring financial institutions to ensure TDES migration plans are in place to meet the July 2010 deadline.

Interlink acquirers, merchants and other payment system participants need to take special care to ensure that all TDES keys are managed in compliance with *PCI PIN Security Requirements* (available at www.visa.com/pinsecurity). Compliance with the Visa PIN Security and Key Management Program will help minimize member liability in the event of a PIN or key management compromise. Entities that fail to comply with Visa's TDES requirements may subject their Interlink-sponsoring financial institution to fines. Implementing additional security using TDES to protect cardholder PINs enables the Visa and Interlink systems to maintain their promise to provide the most secure and reliable form of payment to consumers.

Derived Unique Key per Transaction Protocol

Most U.S. merchants are currently using single-DES Derived Unique Key per Transaction ("DUKPT") protocol for POS PIN encryption. **No version of single-DES DUKPT meets the July 1, 2010, TDES requirement.** To comply with Visa's global TDES requirements, merchants must migrate to TDES DUKPT or TDES using a unique fixed key or unique master session key protocol per device. For entities converting from single-DES DUKPT to TDES DUKPT, Visa requires that new Base Derivation Key (BDK) components be generated in a compliant manner and that old BDKs used for single-DES DUKPT not be used for TDES DUKPT implementations. This helps ensure that implementations of TDES DUKPT follow the *PCI PIN Security Requirements* for the use of keys for their sole intended purpose.

Encryption and Support Organizations

Interlink Encryption and Support Organizations (ESOs) performing POS PED key loading and key injection services on behalf of merchants are a critical component of a merchant's transition to TDES usage. ESOs manage highly sensitive cryptographic keys on behalf of acquirers, merchants, processors and agents; it is critical that all key management and key loading activities are performed only in compliance with the *PCI PIN Security Requirements*. Acquirers must ensure that any Interlink ESOs being utilized by their sponsored Interlink merchants are properly vetted and registered with Visa. Entities



should contact agentregistration@visa.com with any questions regarding Interlink ESO registration requirements.

Client Impact

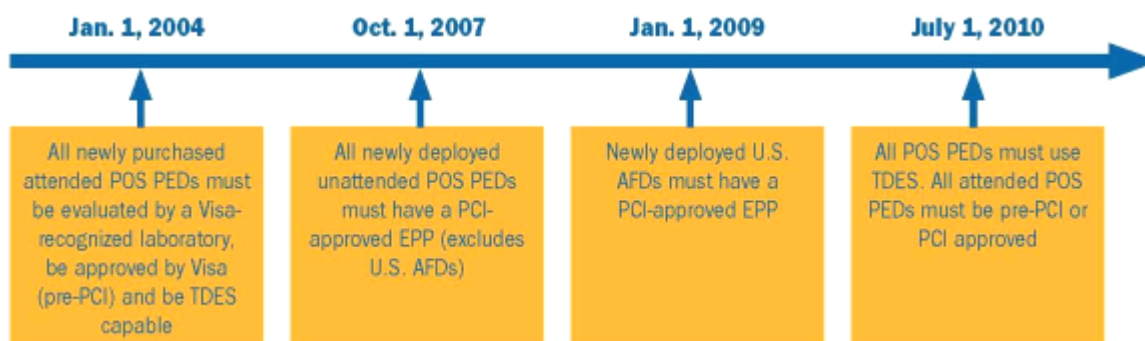
The complete global conversion to POS TDES processing will require upgrades to acquirers', processors', merchants' and payment system participants' host systems and the replacement or upgrade of devices at the point of transaction. The impact of these changes on individual acquirers, merchants and agents will vary, based on the current state of host systems, internal system development costs and the age of currently deployed POS PEDs. Other factors might include impacts on the processing network supporting TDES usage at all POS PEDs.

POS PEDs Required to Support TDES

In 2002, prior to releasing TDES usage requirements, Visa announced that newly purchased POS-based PED hardware must be capable of supporting the TDES algorithm. In conjunction with this POS TDES-capable requirement, the end date for all attended POS PEDs to be TDES capable was announced as July 1, 2010. This was aligned with Visa's PED testing program, which requires that all attended POS PEDs in production to be either pre-PCI or PCI-approved, and all attended and unattended POS PEDs to use TDES by July 1, 2010. Any PED submitted for lab evaluation is tested to ensure it can support TDES. Accordingly, all attended POS PEDs that have never been successfully lab-evaluated and pre-PCI or PCI-approved must be removed from production globally by July 1, 2010.

In 2007, Visa further clarified unattended POS PED requirements and announced requirements for the use of TDES capable and PCI-approved Encrypted PIN Pads (EPPs) within unattended POS PEDs such as Automated Fuel Dispensers (AFDs), kiosks and Unattended Payment Terminals (UPTs). One of the largest numbers of unattended POS PEDs are U.S.-deployed AFDs. When PED testing requirements were first implemented, AFD vendors were unable to meet Visa's PED evaluation requirements for older AFDs deployed in the U.S.; however, AFD vendors have released PCI-approved EPPs for the U.S. marketplace. Recognizing that there were previously no lab-evaluated PEDs for U.S. petroleum merchants to purchase, Visa granted an extension to the January 1, 2004, requirements stating that all newly deployed PEDs must support TDES and be lab-evaluated and Visa-approved. These two requirements have been deferred until January 1, 2009, for U.S. PEDs used in conjunction with AFDs.

Below is the POS PED testing and TDES usage timeline:



Secure TDES Migration Recommendations

To securely migrate to TDES, follow these recommendations:

- Develop detailed plans to migrate to TDES with at least double-length keys.



- In the migration plan, include the conversion of all single-DES DUKPT implementations to TDES DUKPT. Ensure that when converting from single-DES DUKPT to TDES DUKPT, new BDK components are securely generated.
- Contact POS PED vendors, processors and ESOs to establish achievable conversion plan milestones for all organizations.
- Evaluate all encryption zones where PIN translations occur to ensure that each zone in which the PIN travels is TDES encrypted from the point of entry all the way to the issuer. This includes any acquirer zone between a PED and a Host Security Module (“HSM”) where PIN translations occur.
- Ensure that all POS PEDs use encryption keys unique to that device to process PINs.
- Inspect current equipment inventories (e.g., PEDs, key loading/injection devices and hardware security modules) to determine which equipment currently supports TDES (with at least double-length keys) and which equipment needs to be upgraded or replaced.
- Ensure that POS PED inventories and new equipment purchases are in compliance with Visa PED testing requirements. A copy of these requirements can be found at www.visa.com/pin.
- Contact your processors and POS ESOs to ensure that these entities support TDES-compliant key management controls.
- Target known compromised POS PEDs for replacement first. Visa has published known compromised POS PEDs in a November 2007 Security Alert posted on www.visa.com/cisp.
- All attended POS PEDs that have never been successfully lab-evaluated and pre-PCI or PCI-approved must be removed from production globally by July 1, 2010. All payment system participants must determine whether any attended vendor-attested POS PEDs are in use; if so, these PEDs must be retired by July 1, 2010.
- Ensure compliance with the *PCI PIN Security Requirements*.

Related Information

Additional information on TDES, as well as *PCI PIN Security Requirements*, Key Management and PED security, may be found in the following Visa publications and on Visa websites. In addition, Visa offers ongoing Key Management Workshops. For more information on these workshops, e-mail pinusa@visa.com.

Web Resources:

- For a listing of Visa's global TDES usage mandates go to www.visa.com/pin.
- For the *PCI PIN Security Requirements* manual and the *Visa Auditor's Guide to PIN Security* go to www.visa.com/pinsecurity.
- For the most recent listing of PCI-approved PIN-entry devices and other testing and PED security program information, visit www.pcisecuritystandards.org/pin.
- For *PCI POS* and *EPP PIN Entry Device Security Requirements* manuals, visit www.pcisecuritystandards.org/pin.

Publications:

- “POS PIIN Entry Device Vulnerabilities Data Security Alert” in the November 19, 2007, *Data Security Alert* available at www.visa.com/cisp.
- “Risks Affecting Petroleum Merchants Data Security Alert” in the November 17, 2006, *Data Security Alert* available at www.visa.com/cisp.

For More Information

Contact your Visa Account Executive or e-mail pinusa@visa.com.