Seminarios por Internet para Destacar la Seguridad del PIN y de los Datos del Tarjetahabiente por parte de los Comercios

Febrero 12, 2013 (Español)

February 13, 2013 (English)

Limitación de Responsabilidad

- La información, recomendaciones o “mejores prácticas” contenidas en el presente se proporcionan “TAL CUAL ESTÁN”, son mero título informativo y no deberá dependerse de ellas para asesoramiento operativo, de mercadeo, legal, técnico, impositivo, financiero o de otro tipo. Al implementar una estrategia o práctica nueva, deberá consultar con su asesor legal a fin de determinar qué leyes y reglamentaciones son de aplicación según sus circunstancias específicas. Los costos, ahorros y beneficios reales de toda recomendación, programa o “mejor práctica” variarán basado en sus necesidades comerciales y requisitos de programas específicos. Por su naturaleza, las recomendaciones no son garantía de desempeño o resultados futuros y están sujetas a riesgos, incertidumbres y presunciones difíciles de predecir o cuantificar. Nuestras presunciones se hicieron a la luz de nuestra experiencia y percepción de tendencias históricas, condiciones actuales, desarrollos futuros esperados y demás factores que consideramos apropiados según las circunstancias. Las recomendaciones están sujetas a riesgos y a incertidumbres, que podrían hacer que los resultados y tendencias reales y futuros difieran materialmente de las presunciones o recomendaciones. Visa no es responsable por el uso que usted haga de la información contenida en el presente (incluidos errores, omisiones, imprecisiones o falta de oportunidad de cualquier tipo), como así tampoco de presunción o conclusión alguna que usted pudiere inferir de su uso. Visa no otorga garantía alguna, expresa o implícita, y expresamente renuncia a las garantías de comerciabilidad y de adecuacidad de uso para un propósito en particular, a toda garantía de no violación de los derechos de propiedad intelectual de un tercero, a toda garantía de cumplimiento de la información con los requisitos de un cliente o a toda garantía de actualización de la información y de información sin errores. Hasta el grado permitido por la ley de aplicación, Visa no será tenida como responsable ante un cliente o un tercero por daños y perjuicios conforme a teoría alguna de derecho, incluido sin limitaciones, todo daño especial, emergente, incidental o punitivo, como así tampoco por daños y perjuicios por lucro cesante, interrupción de los negocios, pérdida de información comercial u otra pérdida monetaria, incluso si fuere notificada de la posibilidad de dichos daños y perjuicios.

Agenda

- Tendencias de Compromiso y Vulnerabilidades de Seguridad de los Equipos de Ingreso de PIN (PED)
- Repaso de recientes ataques y de las mejores prácticas de prevención
- Repaso de los Mandatos de Uso de PED de Visa
  - Repaso de los Mandatos de Retirada de PED de Visa
- Repaso de las Mejores Prácticas de Uso de PED
- Preguntas y Respuestas

Estrategia de Administración de Riesgo del Sistema de Pago

Fomentar y **mejorar** la confianza de nuestros clientes en Visa como la forma más segura de pagar y cobrar

AVANZAR **Fomentar confianza y estrategias de control de riesgo en los productos y entidades emergentes**

Casos de Alteración de Dispositivos de Ingreso de PIN (PED)

- **La cantidad de casos de alteración de PED está aumentando**
  - Los delincuentes dirigen sus ataques a comercios que tienen ciertos modelos de PED
    - Ataques a PED vulnerables más antiguos y modelos de PED nuevos
    - Modelos inalámbricos se están convirtiendo en el objeto de ataques
  - Ataques van dirigidos a comercios pequeños y grandes, a menudo, múltiples tiendas
    - Intercambian los PED con los PED vulnerados
- **Los ataques son más sofisticados y con mayores adelantos técnicos**
  - Los recientes ataques estaban dirigidos a los modelos de PED *VeriFone Everest,* e *Ingenico i3070*
  - No obstante, nuevos modelos de PED también han sido objeto de ataques
- **Evidencia de que la tecnología se está exportando a nivel mundial**

La alteración de los PED generalmente conlleva:

- Un segundo lector de banda magnética o conexión a un lector existente
- Tarjeta(s) de circuitos adicional(es)
- Membrana de teclado
- Dispositivo Bluetooth
- Chip o unidad de memoria Flash

Alteración de PED en las Américas

Norteamérica

- Ataques en tiendas de cadena con PED más antiguos
- Los PED no están físicamente seguros o protegidos
- Los delincuentes viajan por todo el mercado duplicando los ataques
- Hacen retiros de efectivo en Cajeros Automáticos inmediatamente

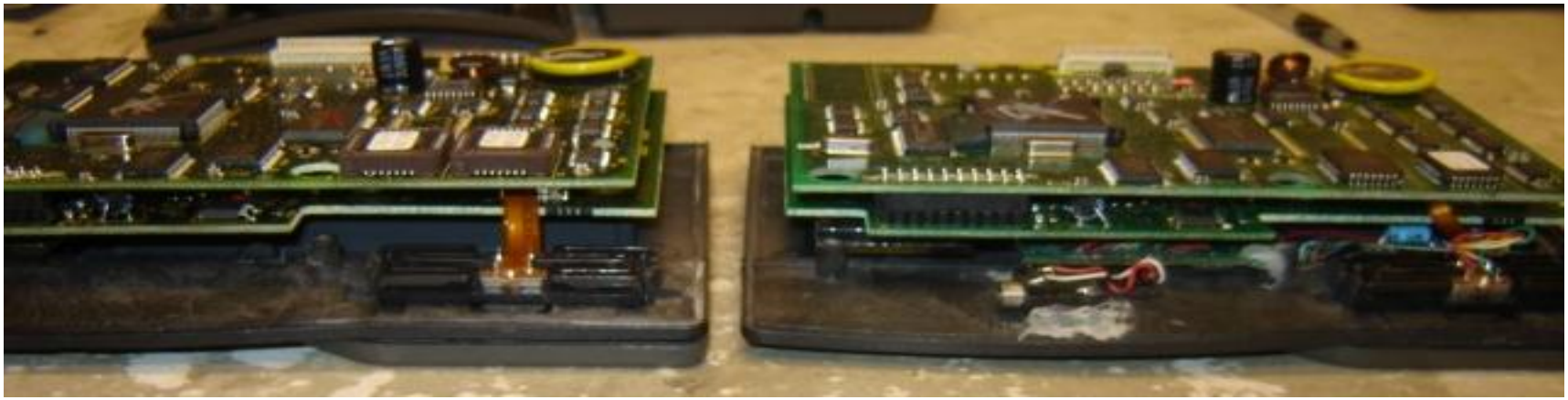
América Latina

- Ataques en Perú, Chile y Colombia
- Ataques sumamente sofisticados
- Los intercambios de PED conllevaban “ingeniería social”
- Se encontraron PED más nuevos aprobados por PCI
- Ataques dirigidos a PED inalámbricos, los cuales resulta difícil asegurar físicamente

VeriFone Everest

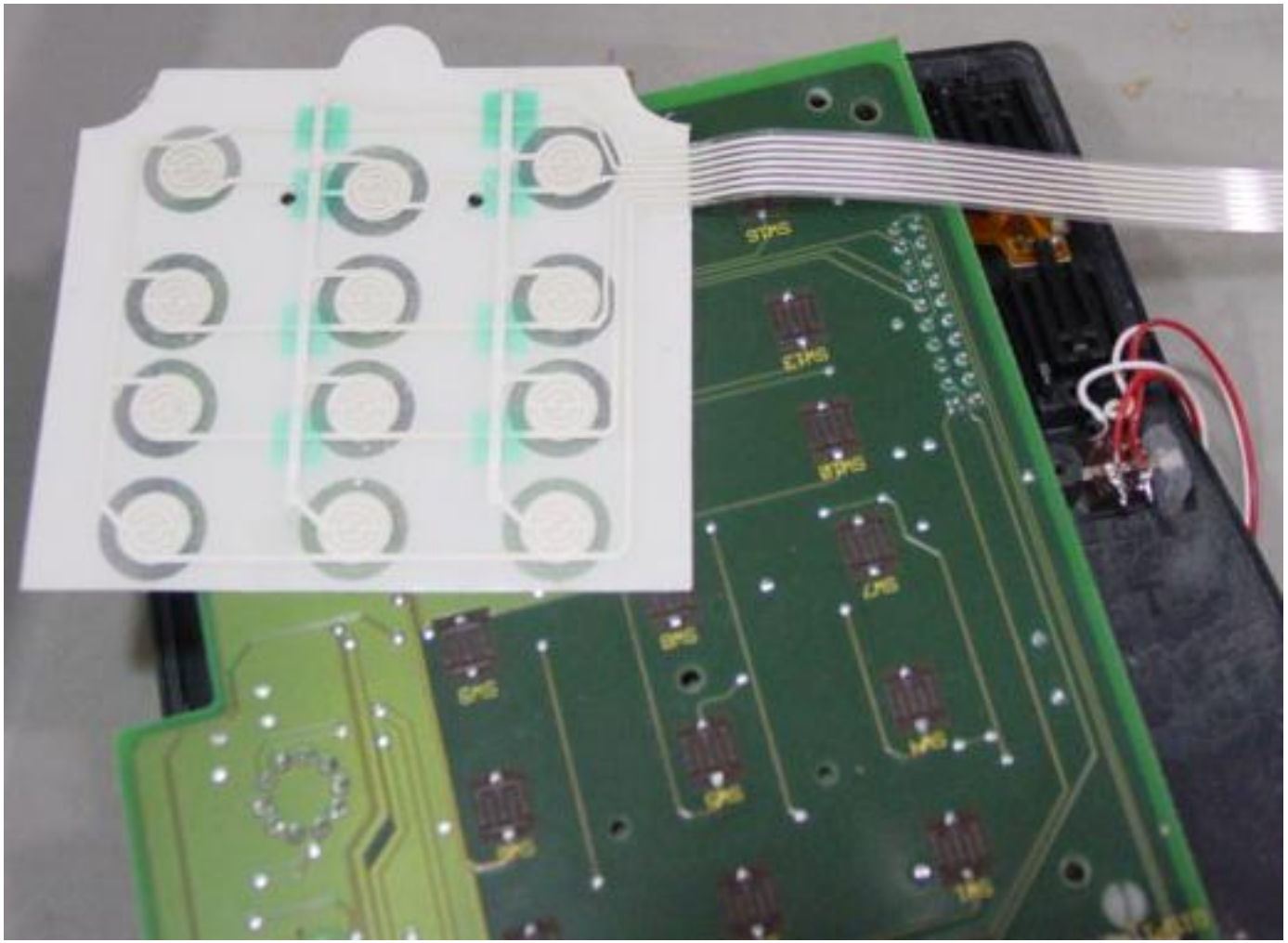
Normal

Alterado



Alteración de PED

Teclado de Membrana para capturar PINs



Medidas Preventivas para Evitar Alteración de los PED

- Sustituir los PED vulnerables cuanto antes posible
- Capacitar al personal para inspeccionar visualmente con regularidad los PED, a fin de identificar cuestiones anormales como
  - Sellos o tornillos que faltan o que han sido alterados
  - Cableado extraño, agujeros en el equipo o la adición de etiquetas
  - Material superpuesto que se utiliza para enmascarar el daño ocasionado por la alteración
- Asegurarse de que los PED estén físicamente seguros / fijados a los mostradores

Repasar las Mejores Prácticas de Visa para el Uso de Terminales:

"La Alteración de los Terminales de Punto de Venta es un Delito… y Usted Puede Evitarlo"

www.visa.com/cisp

VISA

La Alteración de los Terminales de Puntos de Venta. Es un Delito. . . y Usted puede Evitarlo

Cada vez más, los delincuentes con herramientas sofisticadas están dirigiendo sus ataques de forma activa a terminales vulnerables de punto de venta (POS) para robar los datos de las tarjetas de pago y los PINes con fines de fraude mediante la falsificación de la banda magnética. ¡Esa es la mala noticia! La buena noticia es que todos los adquirentes, comercios y procesadores pueden tomar medidas adecuadas para eliminar los puntos débiles de los terminales de POS y evitar la posibilidad de que los equipos de POS sean alterados.

Qué debe Hacer si Detecta Alteración de los PED

- **Contener y limitar inmediatamente la exposición**
  - Remover/desconectar de su red los PED cuya alteración se sospecha
  - Asegurar y salvaguardar todos los PED
  - En los comercios de múltiples cajas registradoras, asociar los PED a cajas / líneas individuales o específicas
  - Los comercios de gran volumen deben tener planes de respuesta a incidentes para hacer frente a los eventos de compromiso
- **Alertar a todas las partes necesarias**
  - Seguir los pasos estipulados en el documento de Visa ***What To Do If Compromised ,*** *en* www.visa.com/cisp
  - Notificar a su banco adquirente y su procesador
  - Notificar al departamento de Control de Fraude de Visa
  - Notificar a su proveedor de PED
  - Los proveedores de PED tienen que notificar al Consejo de Normas de Seguridad de PCI
- **Notificar al equipo de Respuesta a Incidentes de Visa** si no puede comunicarse con su adquirente:
  - **EE.UU.** – (650) 432-2978 o usfraudcontrol@visa.com
  - **Canadá** – (416) 860-3090 o CanadaInvestigations@visa.com
  - **América Latina y el Caribe** – (305) 328-1713 o lacfraudinvestigations@visa.com

Asegurando el sistema de Pagos

El programa de seguridad de datos de Visa maneja la seguridad del sistema de Pagos

Estándares de Seguridad de Datos (PCI DSS)

- Maneja el cumplimiento de PCI DSS para asegurar que las entidades protegen la información del tarjetahabiente

Requerimientos de la Seguridad del PIN PCI

- Cumplimiento avanzado para prevenir los compromisos del PIN.

Programa de Prueba Transacciones de Seguridad del PIN PCI

PCI POS PCI EPP

Estándares de Seguridad de Aplicaciones de Pago PCI (PA-DSS)

- Promueve el desarrollo y uso de las aplicaciones de Pagos seguro.

Lista de Dispositivos de Ingreso de PIN Comprometidos

- Revise los PED en uso para validar si son dispositivos vulnerables conocidos
- *Boletín de Visa* disponible en www.visa.com/cisp
- Tome medidas de precaución para la seguridad de todos los PED en uso o almacenados

VISA

Visa Bulletin

1 September 2011

Compromised PIN-Entry Device Listing Updated; Reminder of Upcoming Mandatory Sunset Dates

Visa has recently identified PIN-entry devices (PEDs) that are susceptible to compromise. Specifically, two hardware versions of the VeriFone Everest Plus PED have been identified in recent compromises:

- VeriFone Everest Plus part numbers P003-400-01, P003-400-02 and P003-400-03 are untested and unapproved. These devices support only single Data Encryption Standard (DES) cryptography and were required to have been retired effective 1 July 2010.
- VeriFone Everest Plus part numbers P003-400-12 and P003-400-013 are pre-Payment Card Industry (PCI) approved. These devices have a **mandatory sunset date of 31 December 2014.**

Both VeriFone Everest Plus point-of-sale (POS) PED hardware versions have been used in tampering and skimming attacks to capture PIN and magnetic-stripe card data. These devices have been compromised in the U.S.; however, this compromise warning is applicable to all deployments. All Visa and Interlink clients must take action to mitigate the risks introduced by these recently compromised POS PEDs.

POS PED Atendidos en Riesgo Conocidos

PED no Evaluados en Laboratorio Comprometidos

Ingenico	VeriFone	Hypercom
eN-Crypt 2400	PINpad 101, 201, 2000	S7S
C2000 Protégé	Everest	S8
	Everest Plus (-0.X)	

Fecha de caducidad obligatoria: Julio de 2010

PED Previos a PCI Comprometidos

Ingenico	VeriFone
eN-Crypt 2100	Everest Plus (-1.X)

Fecha de caducidad obligatoria: Diciembre de 2014 o antes

PCI PED Comprometidos

Ingenico
i3070MP01
i3070EP01

Visa no tiene fechas de caducidad para los PED aprobados en PCI

En www.visa.com/cisp , se encuentra una lista de PED en riesgo

Mejores Prácticas para Comercios Evitar Clonación

1. **Implementar un sistema de autenticación de terminales para detectar cambios internos en los números de serie o de conectividad**
2. **Fijar los terminales / PED a los mostradores para evitar su remoción y asegurar las conexiones de cables**
3. **Inspeccionar y asegurar los PED instalados en líneas de caja de "autopago", no atendidas**
4. **Mantener inventarios precisos de equipos instalados, activos, almacenados o enviados**
5. **Asegurar los PED almacenados y validar el inventario contra los registros de activos**

- www.pcisecuritystandards.org/documents/skimming_prevention_IS.pdf

Categoría de POS PED Atendidos

No Evaluada en Lab- / No aprobado por Visa.

- PEDs Instalados antes de Enero 2004
- Mandatorio por Visa caducan en Julio 2010.

Pre-PCI Aprobados PEDs

- Instalados desde Enero 2004.
- Expira en Dec. 2007
- Caducidad Mandatoria Visa en Dec. 2014
- Listado en: www.visa.com/cisp

PCI Aprobados PEDs

- PEDs instalados desde Dec. 2007
- 253 V1 PEDs expiran en Abril 2014
- Visa no tiene una fecha limite para los PEDS aprobados PCI
- Listados en PCI SSC

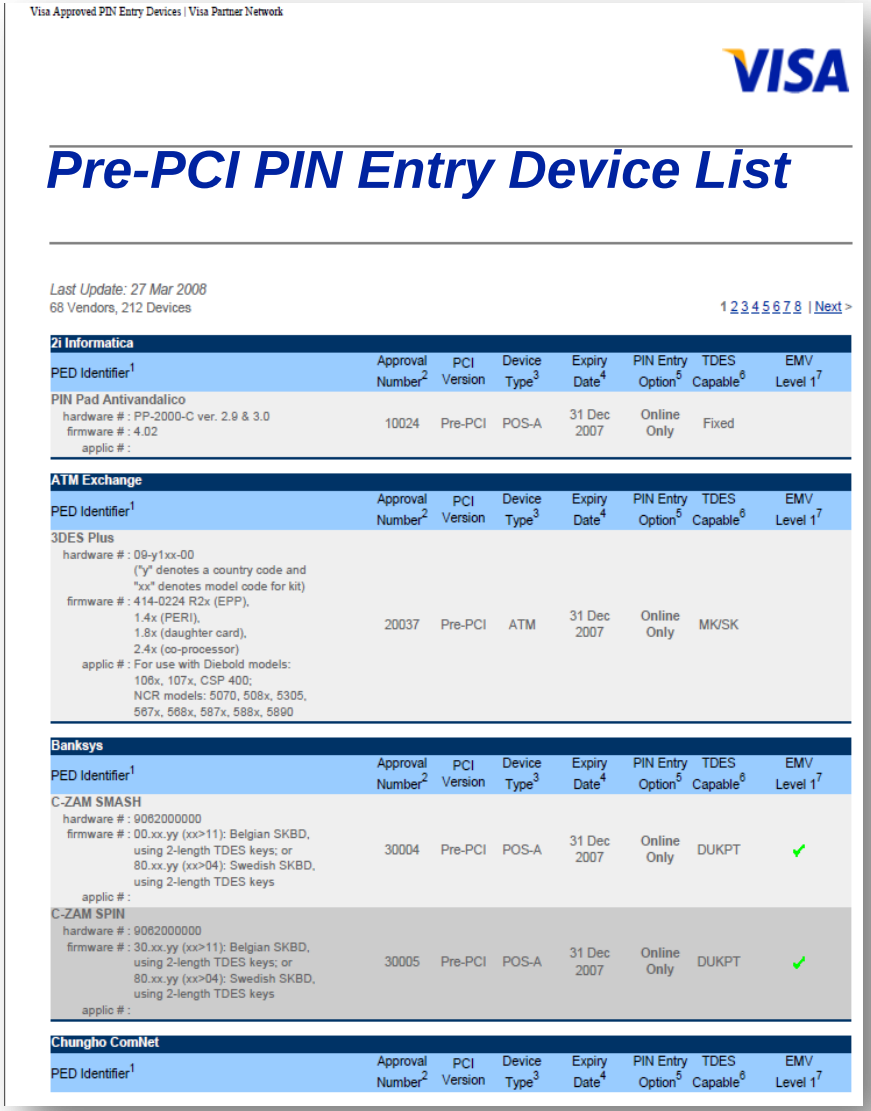
Mejores Practicas para adquisiciones de POS PED:

- **Localizado en el sitio de PED en PCI PTS para validar el estatus de la aprobación.**
- **Mantener impresión de pantalla del PED CCI aprobado con orden de compra**
- **Comprar la ultima versión de PCI PEDs cuando sea posible**

Listado de Dispositivos de PIN Pre-PCI

Reglas de uso Pre-PCI PED

1. **Lista completa de dispositivos que están expirados**
2. **Los PEDs expirados no pueden ser comprados o hacer nuevas instalaciones con ellos.**
3. **Todos los POS PEDS-Pre-PCI deben ser retirados en Diciembre 2014**
4. **Las entidades deben planear para cumplimiento con los mandatos de Visa para fechas de caducidad**
5. **La lista de dispositivos Pre-PCI PIN esta en www.visa.com/pin**



Visa Approved PIN Entry Devices | Visa Partner Network

VISA

Pre-PCI PIN Entry Device List

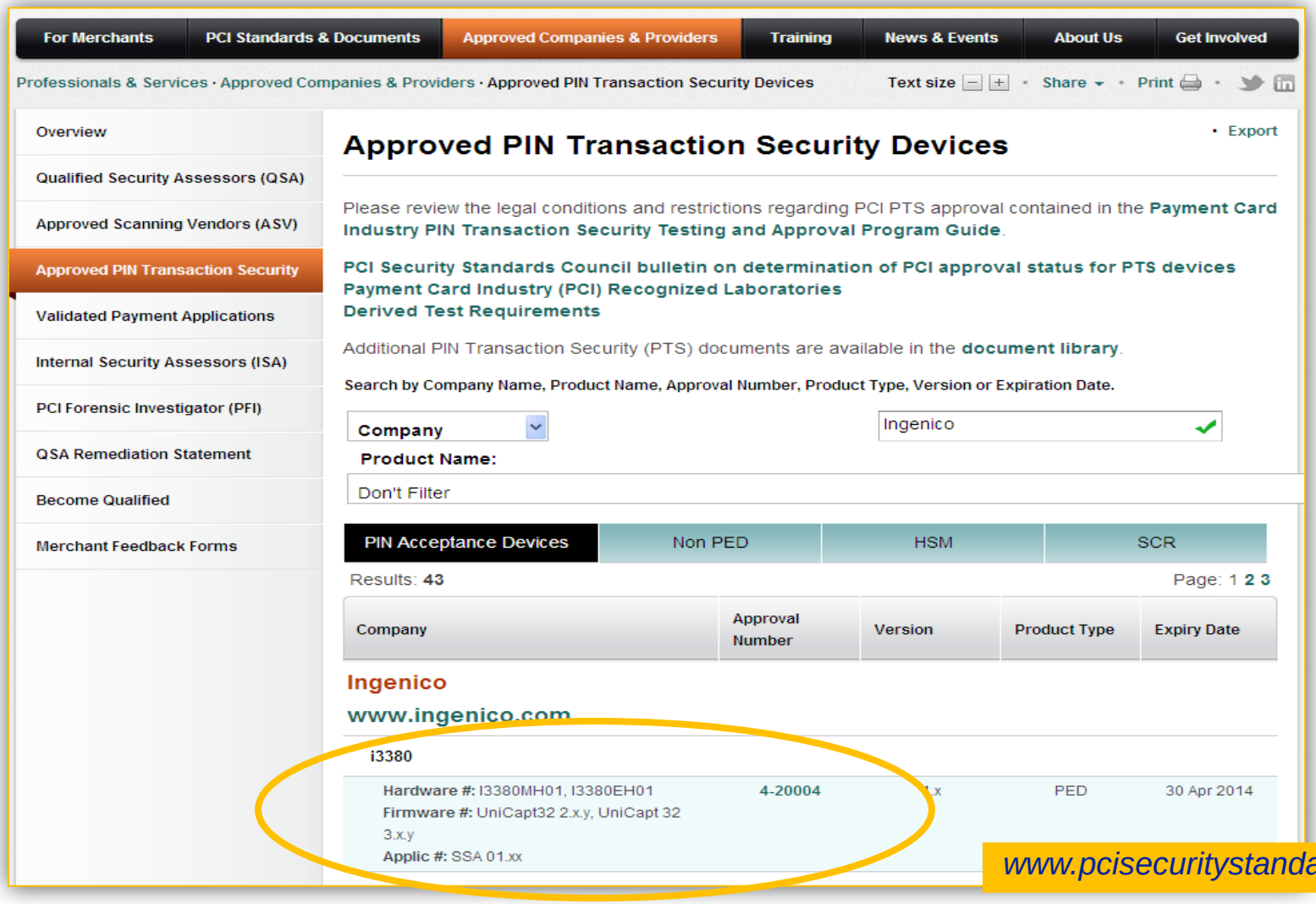
Last Update: 27 Mar 2008
68 Vendors, 212 Devices

1 2 3 4 5 6 7 8 | Next >

PED Identifier[1]	Approval Number[2]	PCI Version	Device Type[3]	Expiry Date[4]	PIN Entry Option[5]	TDES Capable[6]	EMV Level 1[7]
2i Informatica							
PIN Pad Antivandalico hardware # : PP-2000-C ver. 2.9 & 3.0 firmware # : 4.02 applic # :	10024	Pre-PCI	POS-A	31 Dec 2007	Online Only	Fixed	
ATM Exchange							
3DES Plus hardware # : 09-y1xx-00 ("y" denotes a country code and "xx" denotes model code for kit) firmware # : 414-0224 R2x (EPP), 1.4x (PERI), 1.8x (daughter card), 2.4x (co-processor) applic # : For use with Diebold models: 106x, 107x, CSP 400; NCR models: 5070, 508x, 5305, 567x, 568x, 587x, 588x, 5890	20037	Pre-PCI	ATM	31 Dec 2007	Online Only	MK/SK	
Banksys							
C-ZAM SMASH hardware # : 9062000000 firmware # : 00.xx.yy (xx>11): Belgian SKBD, using 2-length TDES keys; or 80.xx.yy (xx>04): Swedish SKBD, using 2-length TDES keys applic # :	30004	Pre-PCI	POS-A	31 Dec 2007	Online Only	DUKPT	✔
C-ZAM SPIN hardware # : 9062000000 firmware # : 30.xx.yy (xx>11): Belgian SKBD, using 2-length TDES keys; or 80.xx.yy (xx>04): Swedish SKBD, using 2-length TDES keys applic # :	30005	Pre-PCI	POS-A	31 Dec 2007	Online Only	DUKPT	✔
Chungho ComNet							

Dispositivos de Seguridad de Transacciones con PIN Aprobados por PCI

- Siempre valide el Hardware, el Firmware y la Aplicación antes de realizar una compra



www.pcisecuritystandards.org

Adquisiciones, Planificación y Uso de PED en POS

- Siempre trate de comprar la versión de PED más reciente
- Nunca compre ni implemente PED vencidos
- Planifique ahora para la próxima fecha de vencimiento de PED
- Tenga en cuenta las 'ofertas' a medida que se acerca la fecha
- Antes de diciembre de 2014, se deben retirar todos los PED en POS atendidos anteriores a la PCI
- Para obtener más información, consulte ***Preguntas Frecuentes Generales sobre PED de Visa***
  - *www.visa.com/cisp*

Dispositivos de Ingreso de PIN Aprobados por PCI

www.pcisecuritystandards.org

Versión de PED de PCI	V1	V2	V3
PED/EPP	261	191	32
Vencimiento de PED de PCI	4/2014	4/2017	4/2020

Requerimientos PCI PIN para el uso seguro de PEDs

PCI SSC fue actualizado con los requerimientos de ***PCI Seguridad del PIN en*** 2011

- Nuevo lenguaje fue adicionado a la seguridad del PIN PCI en el *Requerimiento* 29
- Protección Física y Lógica deben existir para los PEDs instalados
- Precauciones deben incluir :
  - Físicamente montados o atados para prevenir ser removidos.
  - Implementar un sistema de autenticación del terminal.
- La fecha efectiva de Visa para los nuevos requerimientos de PIN PCI fue en Julio del 2012

Modificaciones PCI PIN – Sumario de Cambios

PCI Security Standards Council

Requirement	Section(s)	Modification
25	Main Body Normative Annex B	▪ Clarified that no other person (not similarly entrusted with that component) can observe or otherwise obtain the component. ▪ Specified that key custodians sufficient to form the necessary threshold to create a key must not directly report to the same individual.
	Normative Annex A	Increased minimum pass phrase from six to eight characters for Certification and Registration Authority relevant equipment.
	Normative Annex A	Added biometrics as an associated usage authentication mechanism for security tokens
26	N/A	N/A
27	N/A	N/A
28	N/A	N/A
29	Main Body Normative Annex B	Specified that precautions must be taken to minimize the threat of compromise of PIN-processing equipment once deployed.
	Normative Annex B	Specified that secure areas must be established for the inventory of PEDs that have not had keys injected.
30	N/A	N/A

Anuncios de Chip en Visa

Considerar los mandamientos de Visa en Chip para las nuevas inversiones en actualización de Dispositivos

1	**Programa de Innovación Tecnológica**	Comenzando desde Octubre 2012, Visa eliminara la necesidad de los comercios ser elegibles para la validación anual con PCI DSS para cualquier ano en donde mas del 75 % de las transacciones sean originadas en dispositivos Chip
2	**Desarrollar Infraestructura Procesamiento en Chip**	Para abril 2013 Visa requerirá a los procesadores dar soporte a la aceptación de transacciones Chip en EEUU
3	**Establecer Cambio de Responsabilidad**	Para Octubre 2015 en EEUU adquirentes y comercios que no den soporte a los datos dinámicos de Chip serán contra cargados por fraude de falsificación

Aceptación de POS Futuras

- **Manténgase al corriente de las amenazas emergentes al invertir en el equipo más seguro**
- **Disposiciones de uso/retiro de PED**

Adquisición de PED Seguros, Uso y Planificación

Adquisiciones

- Nunca comprar PEDs expirados
- Siempre comprar versiones 3 de PEDs aprobados por PCI
- Comprar PEDs que tenga capacidad EMV .

Uso

- Asegurar los PEDs que están en comercios
- Use un sistema de autenticación del terminal
- Reemplace los PEDs vulnerables
- Seguimiento al inventario de PEDs

Planificación

- Retire los PEDs POS atendidos Pre-PCI antes de Diciembre 2014

Entrenamientos de Seguridad del PIN

Calendario 2013 :

- **Seguridad del PIN y Manejo de agentes Plus**
  - Febrero 19, Scottsdale, AZ (En Ingles)
- **Manejo de llaves de la Seguridad del Pin y Validación del cumplimiento**
  - Marzo 25 – 27, San Paulo, Brasil (Portugués)
  - Abril 23 - 25, Ashburn, VA (Ingles)
- **Seguridad del Pin y Manejo de llaves**
  - Junio 25, Toronto, Canada (Ingles)
  - Septiembre 10, Ashburn, VA (Ingles)

Para mas información ir a www.visa.com/cisp

- Entrenamientos son acreditados para Educación Continua de Profesional
- Sesiones personalizada en sitio disponibles
- Contacto: VisaBusinessSchool@visa.com

Para Obtener Más Información sobre Seguridad del PIN de Visa

- ***www.visa.com/cisp***
- Boletín de POS PED en Riesgo
- *Lista de PED Previos a PCI*
- *Marco de Validación de Cumplimiento del PIN*
- *Boletín sobre la Política TDES de Visa*
  - *Plataforma para Seminarios por Internet sobre TDES Disponible*
- *Preguntas Frecuentes sobre US POS TDES de Visa*
- *Preguntas Frecuentes sobre PED de Visa*
- *Herramientas de Seguridad del PIN y Mejores Prácticas para Comercios de Visa*
- *Programa de Seguridad del PIN de Visa: Guía del Auditor*
- Otros Boletines e información relacionados con la seguridad del PIN
- Lista internacional de ESO: www.visa.com/merchants/risk_management

Contacto: pinlac@visa.com

Información sobre Normas de Seguridad de PCI PIN y PTS

Consejo de Normas de Seguridad de PCI

- www.pcisecuritystandards.org
  - Nuevos *Requisitos de Seguridad del PIN de PCI*
    - *En vigencia a partir del 1 de Julio de 2012 para clientes de Visa*
  - *Requisitos de Seguridad de los Dispositivos de Ingreso del PIN en PCI POS*
  - *Requisitos de Seguridad de PCI EPP*
  - Lista de Dispositivos de Ingreso de PIN Aprobada para PIN PTS
    - Cientos de Proveedores
    - 490 PED, pero trate de adquirir PED V3 únicamente