Cómo sacar rendimiento al PCI DSS

Zane Ryan, Dot Force
Director General
Tlf. +34 93 656 74 00
Email: zane.ryan@dotforce.es

Bruce Mac Nab, SafeNet
Responsable Comercial & Regional España, Francia y Portugal
Tlf. +33 1 47 55 74 77
Email: bmacnab@fr.safenet-inc.com

Agenda

- Solamente cumplir con las normas o ir más allá…
- Sacar el mayor provecho de la inversión.
- Ejemplos de cómo se puede incrementar el valor de la inversión.
- Un par de ejemplos concretos.

El Valor de Dot Force

Proveer soluciones que estrechan la relación entre empresas y clientes a través de medios electrónicos de manera segura que al mismo tiempo mejoran los procesos online, reducen costes, mejoran los servicios, incrementan la productividad y aumentan el valor.

Confianza es negocio

- **Sin Confianza no hay Negocio**
- **Sin e-Confianza tampoco hay Negocio**
- **Sin e-Confianza tampoco hay e-Negocio**

El porqué de PCI DSS

- **Ladrones**

- **Confianza**

By complying with the PCI Data Security Standard, merchants and service providers not only meet their obligations to the payment system, but also gain the ability to *promote* their business as adhering to the highest security standards established for handling sensitive cardholder data. Customers demand complete assurance that their account information is safeguarded from all possible threats, and where they *put their trust, and their money*, will be based on a merchant's *reputation* for providing a *safe and secure* place to do business.

Fuente: PCI - DSS

Cumplir y nada más o Cumplir y más

- **Tan solo seguir las normas de circulación no convierte al conductor en un conductor seguro**
- **Aún así ser un conductor seguro no prevee ciertas amenazas o riesgos – ¿Sí o No?**
- **Cumpliendo solamente con las normas de fabricación de coches no se hacen los coches más seguros**
- **¿Qué opciones de seguridad quiere Vd. para su coche?**

Los principios básicos de PCI DSS

- **Desarrollar y mantener una red segura**

  1. Instalar y mantener un Firewall para proteger los datos
  2. No usar las contraseñas y otros parámetros de seguridad suministrados por los fabricantes

- **Proteger los datos de los titulares de las tarjetas**

  3. Proteger los datos guardados
  4. Cifrar las transmisiones de los datos e información sensible por las redes públicas

- **Mantener un programa de gestión de vulnerabilidades**

  5. Utilizar y regularmente actualizar el software de Antivirus
  6. Desarrollar y mantener sistemas y aplicaciones seguras

Los principios pricinpales de PCI DSS

- **Implantar medidas estrictas de control de acceso**

  7. Restringir los acceso a los datos según necesidad
  8. Asignar una identificación única a cada persona con acceso a los sistemas
  9. Restringir al acceso físico a los datos

- **Regularmente monitorizar y probar la seguridad de las redes**

  10. Rastrear y monitorizar todos los accesos a los recursos de la red y los datos de los titulares de las tarjetas
  11. Regularmente probar la seguridad de los sistemas y los procesos

- **Mantener una política de seguridad de la información**

  12. Mantener una política que trate de todas las cuestiones de la seguridad informática

Preguntas para ver más allá de PCI - DSS

Requisito	Pregunta	Posible solución
1. Montar un Firewall de red	¿Llega a analizar paquetes de OSI 5, 6 y 7?	IPS y/o WAF
2. No utilizar las contraseñas por defecto de los fabricantes	¿Se pueden detectar automáticamente firmas de vulnerabilidades conocidas?	Sistemas de autenticación de dos factores, IPS y/o WAF
3. Proteger los datos de las tarjetas y de los titulares de las tarjetas guardados	¿La base de datos está cifrada?	Programas de cifrado de datos
	¿El acceso desde la aplicación Web a la base de datos es directa?	Separar las aplicaciones desde el servidor con la base de datos con Firewall y/o HSM
	¿Qué protección hay contra fugas de información?	Detectar y bloquear la salida de información sensible (WAF)

Preguntas para mirar más allá de PCI - DSS

Requisito	Pregunta	Posible solución
4. Cifrar las comunicaciones	¿Cómo se asegura de que el uso de un protocolo de cifrado es suficiente fuerte?	Control de calidad
	¿Se cifran las sesiones de comunicación?	Cifrado de SSL o TLS y cifrado de correo-e
	¿Si, se cifran las comunicaciones con SSL, ¿Cómo se puede analizar los paquetes cifrados?	IPS y WAF con capacidad de analizar paquetes cifrados con SSL
	¿Se cifran todas las comunicaciones entre las aplicaciones y los sistemas de back-end?	Cifradores de conexiones de red
	¿Se cifran los accesos de los administradores a las aplicaciones?	SSL, TLS, VPN
5. Desplegar software de Antivirus	¿Se detectan los virus en E-mail, IM, la red?	Antispam, AntispIM, IPS, WAF
	¿Se detectan los troyanos y acceso a través de puertas traseras? (WAF)	Antispam, AntispIM, IPS, WAF
	¿Se pueden entrar a través de navegación en páginas Web no deseadas?	Filtrado de URL (Tiempo real o bases de datos históricas)

Preguntas para mirar más allá de PCI - DSS

Requisito	Pregunta	Posible solución
6. Desarrollar y mantener sistemas y aplicaciones seguras	¿Cómo se detectan los ataques?	IPS con capacidad de analizar y catalogar el comportamiento (negative security model)
	¿Cómo se detectan la aparición de una nueva aplicación en la red?	IPS y/o pasarelas de seguridad para la mensajería instantánea (MI)
	¿Cómo se detectan la aparición de un nuevo equipo en la red?	IPS y/o pasarelas de seguridad para la MI
	¿Existe un Inventario completo (en tiempo real) de todas la aplicaciones y equipos en la red?	IPS y/o pasarelas de seguridad para la MI
	¿Se detectan cambios en las aplicaciones?	WAF
	¿Se detectan imperfectos o vulnerabilidades en las aplicaciones?	WAF con capacidad de catalogar el comportamiento de aplicaciones (positive secuirty model)
	¿Se puede proteger la aplicación contra vulnerabilidades sin reescribir la aplicación?	WAF
	¿La aplicación está desarrollada con código seguro?	WAF y HSM
	¿Qué control de calidad de la aplicación existe?	Software de pruebas de calidad, y pruebas de penetración, WAF y IPS

Preguntas para ver más allá de PCI - DSS

Requisito	Pregunta	Posible solución
7. Restringir el acceso a los datos de las tarjetas	¿El acceso es con contraseñas?	Llaves de autenticación, tarjetas inteligentes con certificados, biometría
	¿Hay algún control más allá de la autenticación de usuario?	NAC a veces incorporado en IPS (Perfil de usuario, dir. IP, MAC, configuración del PC)
	¿El acceso desde la aplicación a la base de datos es directa?	HSM
8. Gestión de usuarios Asignar una identidad única para cada usuario	¿Cómo se audita el acceso por usuario?	NAC, IPS, WAF, HSM
	¿Cómo se audita el uso de los programas por usuarios?	NAC, WAF
9. Acceso físico	¿Está físicamente separado y controlado?	Salas protegidas de máquinas y HSMs

Preguntas para mirar más allá de PCI - DSS

Requisito	Pregunta	Posible solución
10. Rastrear y monitorizar todos los acceso a los datos de las tarjetas	¿Cómo se monitoriza el acceso a los recursos de la red y los datos de las tarjetas?	HSM, NAC, IPS, WAF
	¿Cómo se monitoriza qué información sale de la aplicación - Números de tarjetas?	WAF
	¿Cómo se previene la fuga de información?	HSM, WAF, control de dispositivos externos
	¿Qué política hay para informar sobre todos los accesos y usos de los datos de las tarjetas?.	HSM, NAC, WAF
11. Pruebas frecuentes	¿Se hacen pruebas de penetración periódicamente?	Consultores de seguridad
	¿Se dispone de herramientas de escaneo y detección de vulnerabilidades?	Aplicaciones de escaneo de vulnerabilidades
	¿Se disponen de herramientas de escaneo y detección de vulnerabilidades en tiempo real?	WAF
12. Mantener una política de seguridad	¿Hay sistemas que aseguran el cumplimiento según la política de la seguridad de las aplicaciones en la organización	HSM, WAF entre otros

SafeNet : Una perspectiva de clientes

Bruce Mac Nab

SafeNet
The Foundation of Information Security

Agenda

- Quiénes somos?
- Qué hacemos?
- Las empresas que confian en nosotros
- Nuestra collaboracion a cumplir con PCI DSS
- Ejemplos de conformidad con PCI DSS

SafeNet: Expertos en seguridad desde hace 23 años

- **Expertos en seguridad desde hace 23 años:**
  - Comunicaciones
  - Propiedad Intelectual numérica
  - Datos e Identidades digitales
- **Ingresos en 2006: $293 millones**
- **Empleados**
  - 1050 empleados con mas de 350 ingenieros expertos en criptografía
- **Liderazgo en los sectores con los requisitos más exigentes en seguridad:**
  - El sector financiero
    - SafeNet HSMs tiene 7.600 asociados de SWIFT
  - Protección de Identidades
    - Los HSMs de SafeNet protegen los sistemas de los pasaportes electrónicos de más de 30 países

Historia de adquisiciones

El portafolio de soluciones de SafeNet
Gestión de identidades

IDENTITIES

Authentication, Remote Access, and Compliance Enforcement Products

ID Tokens and Middleware

- Borderless Security 330 Smartcard
- Borderless Security iKey 1000 and 2032 (USB token)
- Borderless Security Single Sign On
- Borderless Security Core
- Management System

ID Management

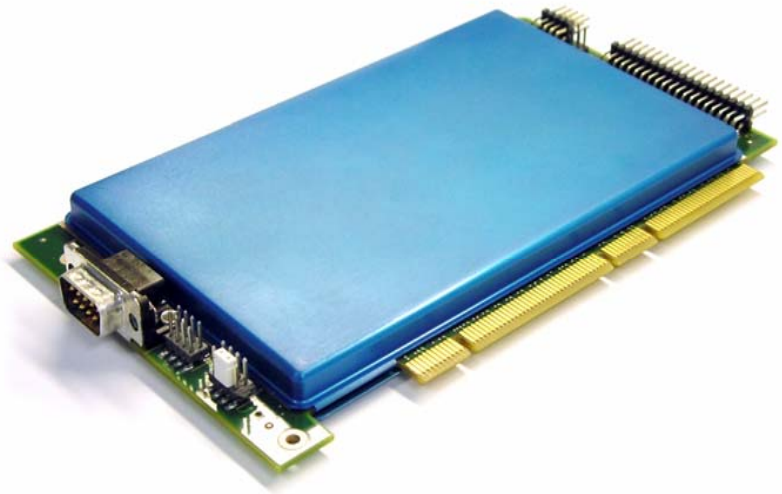
- Luna HSM
- Protect Host
- Protect Server
- API Toolkits
- Command Interfaces

RAINBOW TECHNOLOGIES

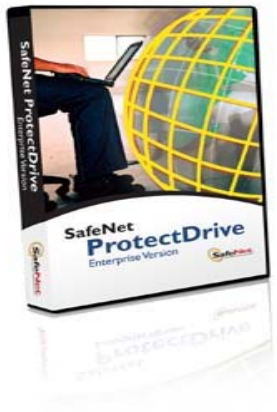
DATAKEY

CHRYSALIS-ITS ULTIMATE TRUST

eracom TECHNOLOGIES



El portafolio de soluciones de SafeNet
Cifrado y portección de datos



COMMUNICATIONS

Encryption Products

Data in Motion – Bulk Encryption
- Ethernet Encryptor
- SONET / SDH Encryptor
- ATM/Frame/Link Encryptors

Data in Motion – Remote Access
- High Assurance IPSec Gateways
- High Assurance VPN Clients
- Borderless Security SSL iGate (SSL VPN)

Policy Management
- Security Management Center

Data at Rest
- ProtectDrive
- ProtectFile
- Protect Pack

CYLINK®

El portafolio de soluciones de SafeNet
Protección de propiedad intelectual (DRM) y soluciones empotradas (OEM)

IDENTITIES

Authentication, Remote Access, and Compliance Enforcement Products

ID Tokens and Middleware
- Borderless Security 330 Smartcard
- Borderless Security iKey 1000 and 2032 (USB token)
- Borderless Security Single Sign On
- Borderless Security Carc
- Management System

ID Management
- Luna HSM
- Protect Host
- Protect Server
- API Toolkits
- Command Interfaces

COMMUNICATIONS

Encryption Products

Data in Motion – Bulk Encryption
- Ethernet Encryptor
- SONET / SDH Encryptor
- ATM/Frame/Link Encryptors

Data in Motion – Remote Access
- High Assurance IPSec Gateways
- High Assurance VPN Clients
- Borderless Security SSL iGate (SSL VPN)

Policy Management
- Security Management Center

Data at Rest
- ProtectDrive
- ProtectFile
- Protect Pack

INTELLECTUAL PROPERTY

Rights Management Products

Anti-Piracy and License Management
- Sentinel RMS
- Sentinel Hardware Keys
- Unified Software Protection

Content Protection
- MediaSentry services

Digital Rights Management
- DRM Mobile
- DRM Fusion

EMBEDDED SECURITY PRODUCTS FOR OEMs

VPN/IPS/FW Software
QuickSec for Unified, Unified IPSec, Unified Anti-Virus, Telecom, IKEv2,

Semiconductor IP
SafeXcel IP Security Engines

Global Top 100 – SafeNet Protege

■ 3M Corporation ■ Abbott Laboratories ■ American Express ■ Amgen ■ Bank of America ■ Barclays ■ BBVA-Banco Bilbao Vizcaya ■ BNP Paribas ■ BP ■ ChevronTexaco ■ Cisco Systems ■ Citigroup ■ Coca-Cola ■ Comcast ■ ConocoPhillips ■ Dell ■ Dow Chemical ■ EI du Pont de Nemours ■ Exxon Mobil ■ FannieMae ■ France Telecom ■ General Electric ■ Goldman Sachs ■ HBOS ■ Hewlett-Packard ■ HSBC ■ IBM ■ ING Group ■ Intel ■ Johnson & Johnson ■ Lloyds TSB Bank ■ Medtronic ■ Merck & Co ■ Merrill Lynch ■ Microsoft ■ Morgan Stanley ■ Nokia ■ Novartis Pharma AG ■ Oracle Corporation ■ Pfizer ■ Qualcomm ■ Royal Bank Of Scotland ■ Royal Dutch/Shell Group ■ Samsung Electronics ■ SBC Communications ■ Siemens Group ■ Telefonica ■ Telstra ■ Total Fina Elf ■ Tyco International ■ UBS ■ United Parcel Service ■ Verizon ■ Vodafone ■ Wachovia ■ Wal-Mart ■ Walt Disney ■ Wells Fargo ■

Referencias Españolas

- Banco de España
- Crèdit Andorrà
- Bankinter
- Jyske Bank
- INSA
- Generalitat de Cataluña
- SeMarket
- Endesa
- DHL
- Blumaq
- Colegios de arquitectos
- Petromiralles
- JCyL
- Etc...

Gestión de llaves, Encriptación y PCI

- **Las exigencias del Payment Card Industry Data Security Standard:**
  - Proteger los datos guardados y no guardar datos de tarjetas sin necesidad
  - Cifrar las transmisiones de los datos de los titulares de tarjetas e información sensible enviada por redes públicas
  - Instalar y mantener un Firewall para proteger los datos
  - No usar las contraseñas y otros parámetros de seguridad suministrados por los fabricantes
  - Utilizar y actualizar regularmente el software de Antivirus
  - Desarrollar y mantener sistemas y aplicaciones seguras
  - Restringir los acceso a los datos según necesidad
  - Asignar una identificación única a cada persona con acceso a los sistemas
  - Restringir al acceso físico a los datos
  - Rastrear y monitorizar todos los accesos a los recursos de la red y los datos de los titulares de las tarjetas
  - Regularmente probar la seguridad de los sistemas y los procesos
  - Mantener una política que trate todas las cuestiones de seguridad informática

¿Qué es un HSM?

- **Un Hardware Security Module (HSM) es un módulo criptográfico que consiste en una colección de algoritmos, almacenes seguros de llaves digitales, aceleración de procesos criptográficos y gestión de llaves dentro de una caja negra no modificable – es parecido a un juego de piezas criptográficas de LEGO – cómo se juntan las piezas determina lo que hace el HSM**
  - Una caja fuerte para almacenar seguramente las llaves digitales sensibles
  - Acelera las operaciones criptográficas para eliminar los cuellos de botella
  - Proporciona una estela de auditoría clara y facilita el cumplimiento con los estándares
  - Gama extensa de opciones de seguridad, rendimiento y capacidad de almacenamiento

¿Porqué utilizar HSMs?

- Protegen de ataques internos y externos
- Previenen que las llaves sean vulnerables ante fallos del sistema
- Defienden las llaves de Virus y Troyanos
- Coartan, controlan y protegen las copias de seguridad

Un caso práctico en Inglaterra

COMMIDEA
CARD PAYMENT PROCESSING SYSTEMS

www.commidea.com

Negocio: desarrollador de software de procesamiento de pagos con tarjetas en Inglaterra

Situación: Una auditoria descubre que los códigos de tarjetas no se cifraban

Solución: Implantación de una solución de cifrado de base de datos con una HSM de SafeNet (Luna SA homologado FIPS 140 -2 nivel 3)

Un caso práctico en España

PETROMIRALLES: www.pertomiralles.com

Negocio: En Cataluña encabeza el ranquing de las distribuidoras independientes de combustibles líquidos, ocupando el tercer lugar en todo el estado

Situación: Una auditoria por UTA (emisor alemán de tarjetas de crédito) les obliga a proteger su proceso de autorización de transacciones con HSMs

Solución a corto plazo: Implantación de dos HSMs de Protect Server de SafeNet en alta disponibilidad e integración con la aplicación actual de autorización de pagos para proteger y cifrar todo el proceso de la autorización de las transacciones

Solución a medio plazo: Extender la utilidad del sistema actual a otras tarjetas (VISA, Mastercard, PETROMIRALLES etc….) para cumplir con el PCI DSS

A caso practico global

- **The largest scheduled coach provider in Europe**
  - Operations include bus services in the USA & Canada, ALSA and Continental Auto bus and coach services in Spain
  - Carry over 16 million customers to 1000 destinations every year in the UK
- **Multi-channel sales strategy**
  - Ticket offices and travel agents
  - Call centres
  - Web sites
  - Self-service ticket kiosks
  - Mobile ticketing
- **Strong focus on security**
  - Early adopter of Chip & PIN

National Express and PCI DSS

- Compliance a growing concern for UK businesses
- The Logic Group selected SafeNet to provide the HSMs for its Enhanced Security Solution
- National Express turned to The Logic Group to deliver a solution offering a high level of security without disruption to the business
- Installation of the Enhanced Security Solution was completed within one month from order

Gracias