KEY Management
PCI DSS Reference
Agenda:

- The need for key management
- PCI- Key Management overview.
- Key management – PAIN points.
- Credit card processing solution.
- Key Management architecture case study.
The need for key management

- Protect Data – Encryption \ Signing.
  - Secure Creation of strong keys.
  - Secure usage for Keys.
  - Separation of duties.

**Design for:**
Confidentiality, Integrity & Availability.
PCI & Card Holder Data

- **Apply** to all organizations that store, process or transmit cardholder data.

- **Cardholder account data includes:**
  - *pan* – primary account number, Card holder name, Service code, Expiration date.
  - **Sensitive authentication data includes:**
    - card’s magnetic stripe
    - personal identification numbers – CID/ CVC2/CVV2 … .
    - chip
PCI & Card Holder Data

Types of Data on a Payment Card

- **PAN** (Primary Account Number)
  - 1234

- **Expiration Date**
  - Valid from 02/07 to 02/10

- **CID** (American Express)
  - (data on track 1)

- **CAV2/CID/CVC2/CVV2** (Discover, JCB, MasterCard, Visa)
  - (data on tracks 1 & 2)

- **Magnetic Stripe**
  - 

Cardholder account data includes:
- **Pan** – primary account number, Card holder name, Service code, Expiration date.

Sensitive authentication data includes:
- **Card's magnetic stripe**
- **Personal identification numbers** – CID/ CVC2/ CVV2…
- **Chip**
Requirement 3 – “Protect stored cardholder data”

- Keep cardholder data storage to a minimum.
- Do not store sensitive authentication data after authorization (even if encrypted).
- Mask PAN when displayed: XXXYY******ZZZZ.
- Render PAN, at minimum unreadable anywhere it is stored BY:
  - One-way hashes, Truncation, Index tokens \ pads
PCI requirement 3.5.X

- **3.5** Protect encryption keys used for encryption of cardholder data against both disclosure and misuse.
  - **3.5.1** Restrict Access to keys to the Fewest number of Custodians necessary
  - **3.5.2** Store keys Securely in the fewest possible Locations and forms.
PCI requirement 3.6.X – Encryption Keys

- **3.6** implement all key management
  - **3.6.1** Generation of strong keys
  - **3.6.2** Secure key distribution
  - **3.6.3** Secure key storage
  - **3.6.4** Periodic changing of keys - annually.
  - **3.6.5** Retirement or replacement of old or suspected compromised cryptographic keys
  - **3.6.6** Split knowledge and establishment of dual control.
  - **3.6.7** Prevention of unauthorized substitution of keys
  - **3.6.8** Key custodians need to sign a form.
Key Management – Pain Points

How to?

- **Split knowledge and establishment of dual control** of cryptographic keys.
- Encrypt / decrypt data process.
- Restrict Access to keys.
  - Secure key storage & Prevention of unauthorized substitution of keys.
  - Secure key distribution.
- **Periodic changing** of keys \ compromised.
  - re-encryption.
  - The weakest point – interface with existing \ new application
Credit Card transaction processing and reporting architecture

Credit Card Company

Server TX

Browser

Reporting

Reporting

External FW

VPN

TX Server

Encrypt Configuration file

App User

DB

AD

User

User

User

User
Key Management - Case Study #1

- Only one key
- Symmetric Encryption.
- Split keys:
  - DB
  - FS
- Complex – process to change key.
Case Study #1 - generating & using EK

Key Storage

DPAPI AP

TX server

Reporting server

Key Storage

DB encryption

SQL Server

SM1

SM2

SM3

Key Tool

Policy

© BY. <Yaron Hakon/> 2BSecure.
Case Study #1 - Payment Data TBL

<table>
<thead>
<tr>
<th>Encrypted PAN</th>
<th>ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>2Q3RQERROWDVsdfr36j34356478346346534tnmw46k7qw3234623h6555*%#4tmwrtnehy9w5ty34pot834np c8i347ncbWEGQDQ##@@##@RBQWER7&amp;7&amp;SSDFSADGQWDER$7T23m24Q#VB==9095qsdtv56457vw476v3463463j26462462346234wcv w323vg</td>
<td>1</td>
</tr>
</tbody>
</table>

Key(PAN)

Clear PAN

Reporting server
Case Study #1 - Transactions process

Credit Card Company
Case Study #1 - Reporting process

Get TX Data …

Application needs to control the Access for Clear PAN!
Key Management - Case Study #2

- Master and Session keys.
- Master key - Asymmetric Encryption – X509.
  - Split keys:
    - public
    - private
- Session keys - Symmetric

Advantages:
- **Split knowledge and establishment of dual control.**
- Advantages:
  - process to change key.
  - Add new application.
Case Study #2 – Master & Session Keys

OPEN – U\P

CSO

CEO

SE Engineer

Split Certificate: Public \ Private

Authentication & Authorization

Session Keys - Generate 100 AES -256 symmetric keys in XML format

Master Key Request For Cert

X509 Certificate

Certificate Service

Encrypt Configuration file

Reporting Server

TX server

SQL Server

X509 Certificate - PFX
password protected - private-

X509 Certificate - public-
Case Study #2 – Master & Session Keys

Session Keys – AES -256 symmetric keys in XML format

Encrypt Session Key With Public Master Key

Encrypt PAN with Session Key

Credit Card Company

X509 Certificate - public-

Session Keys

Encrypt Configuration file

Save TX data + Encrypted PAN + Encrypted Session Key

Session Key_X

TX Data input

Server TX

TX server

Credit Card Company

SQL Server

© BY. ©Yaron Hakon/ 2BSecure.
## Case Study #2 - Payment Data TBL

<table>
<thead>
<tr>
<th>Encrypted PAN</th>
<th>Encrypted Session Key</th>
<th>Mask PAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>2Q3RQERRQWDVsdltr36j34356476346346534tntmrw46k7qw32346</td>
<td>WEQDO#@#@RBRQWER*&amp;&amp;&amp;'SSDFSADQCWDER$*T23m24Q/#VB= -9096qsdv156457w4756v3463463j26462462462462344wcv w323vg</td>
<td>1234- XXXXXX- 6789</td>
</tr>
</tbody>
</table>

**Clear PAN**

**Master_Public_Key(Session Key_X)**

**Session_Key_X(PAN)**
Case Study #2 - Reporting Service - Decryption

Get Mask PAN

Get Clear PAN

Authentication & Authorization

Check user Permission for Certificate

Decrypt Session KEY_X with Master Private Key

Decrypt PAN with Session KEY_X

Get TX DATA

User X

Report Server

SSL

2B Secure

© BY. Yaron Hakon/ 2BSecure.
Case Study #2 - Changing the Master Key

<table>
<thead>
<tr>
<th>Encrypted PAN</th>
<th>Encrypted Session Key</th>
<th>Mask PAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>2Q3RQERRROWDVslr36j34356476346346534ttnw46k7qw32346</td>
<td>WEQDQ#@#@#RBRQWER*T23m24Q#VB=9096gsdvl56457w475v3463463j26462462346234wcv w323vg</td>
<td>1234- XXXXXX- 1234</td>
</tr>
</tbody>
</table>

Decryption with Old Master Private Key.

Encryption with New Public Master Key.

X509 Certificate- PFX password protected - private-

X509 Certificate - public-
Questions
Summary

• Need to design Key Management solution.
• Mast Do Separation of duties.
• Plan for Re – Encryption.
  • Consider dawn time.
  • Session key can minimize the RE – encryption dawn time.
• Protect the keys !.
• Protect the client side that has permission to view clear –text data (memory protection).
Additional Resources

- .NET encryption: AES
- .NET DPAPI
- .NET RNGCryptoServiceProvider
Visit my sites at:

http://www.applicationsecurity.co.il/
www.2BSecure.co.il