KEY Management PCI DSS Reference

Yaron Hakon
WAF TEAM LEADER
Application Security Consultant
2BSecure
yaron@2bsecure.co.il

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.

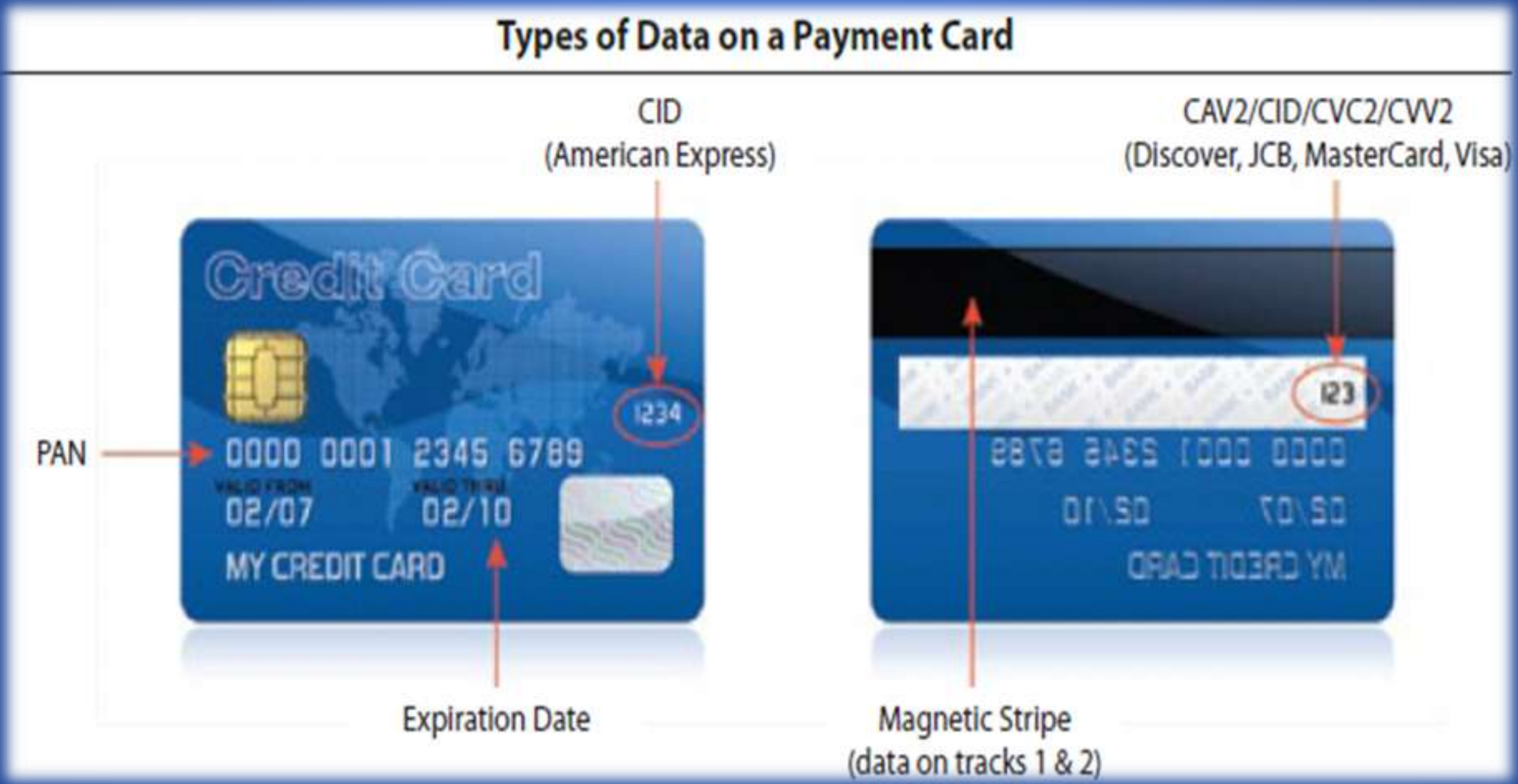
Design for:

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

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: XXXXYY******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

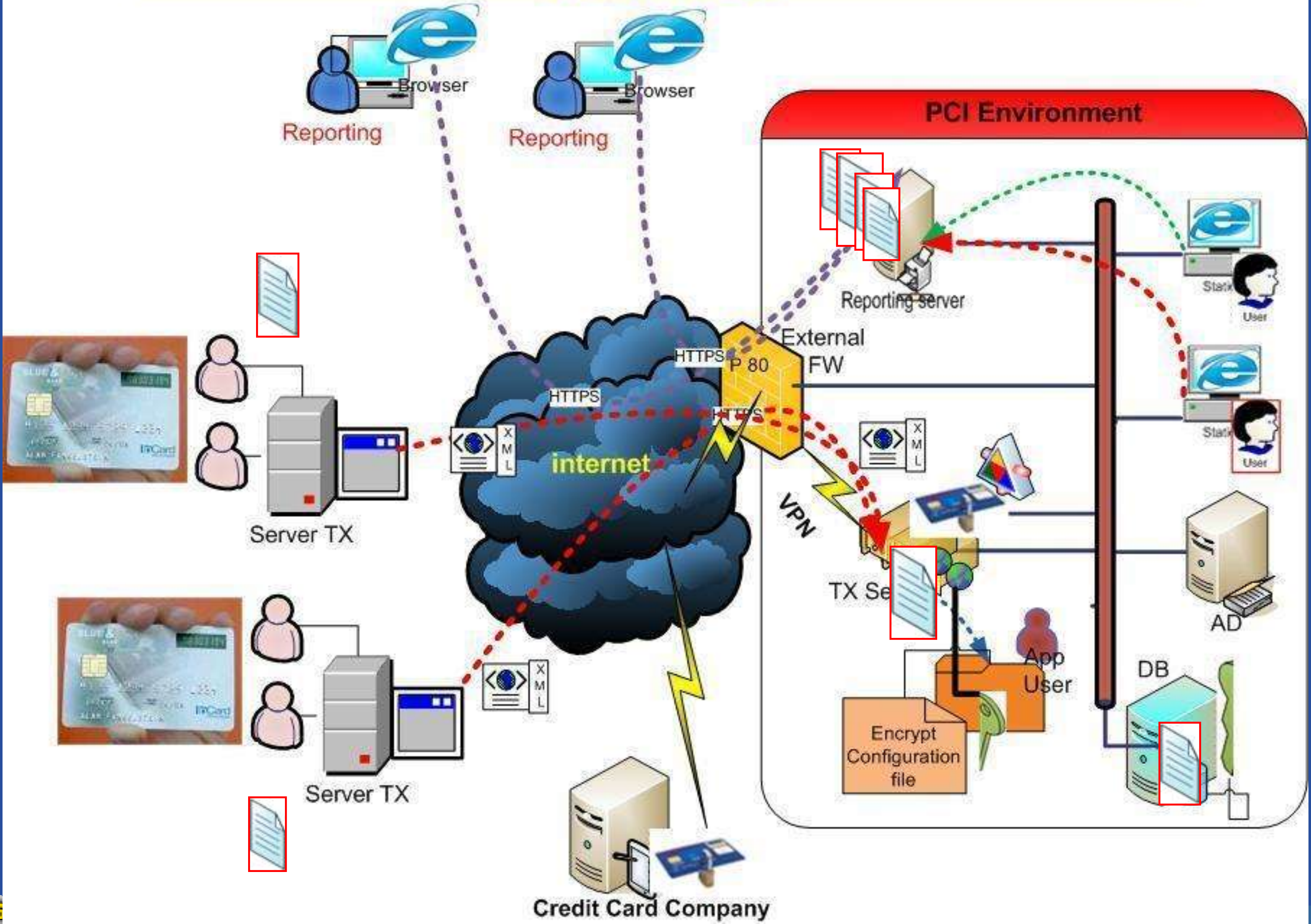
- 3.6 implement all key management
  - 3.6.1 Generation of strong keys
  - 3.6.2 Secure key distribution
  - 3.6.3 Secure key storage
  - 3.6.4 Periodic changing of keys - annually.
  - 3.6.5 Retirement or replacement of old or suspected compromised cryptographic keys
  - **3.6.6 Split knowledge and 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

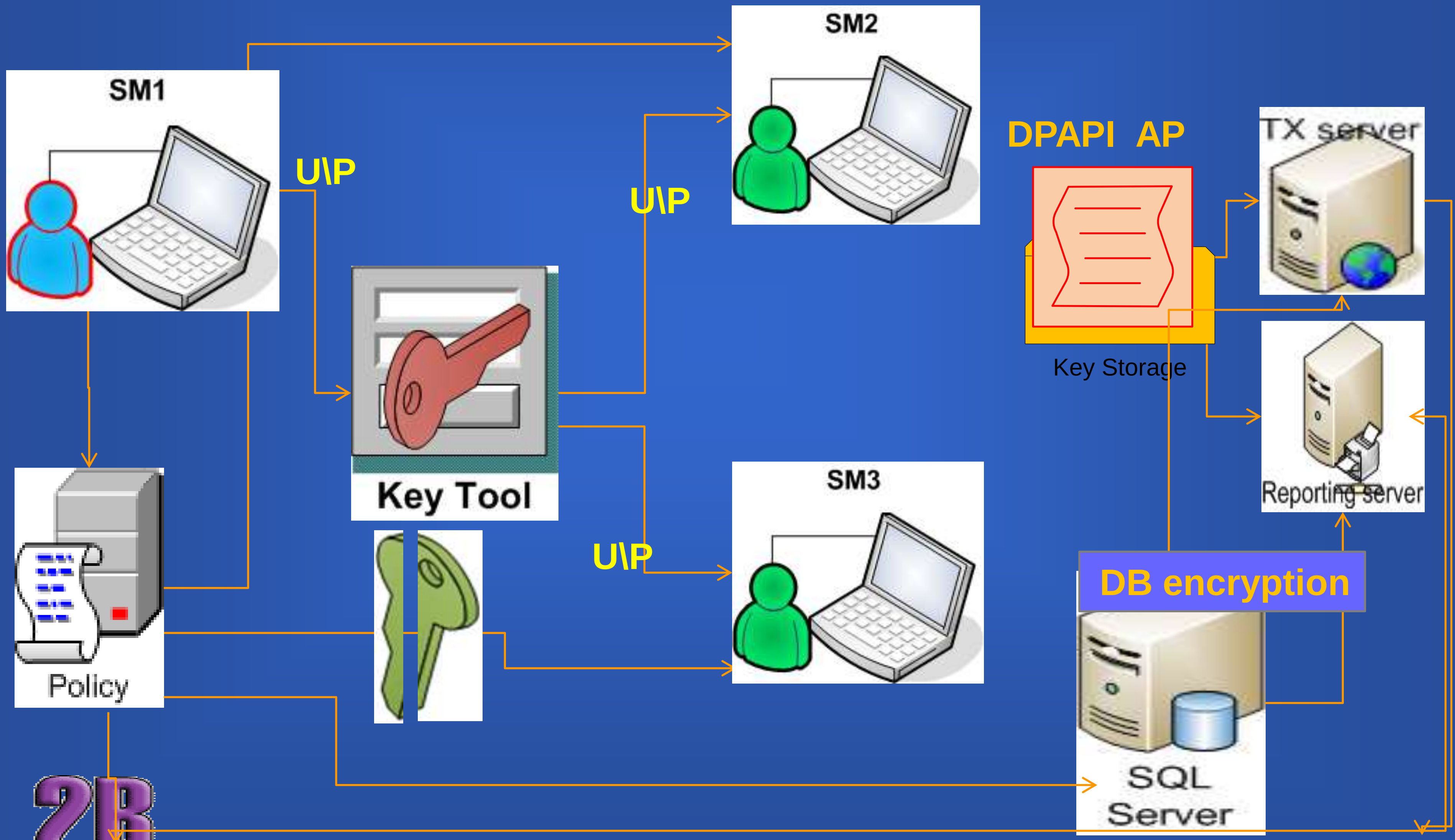


Key Management - Case Study #1

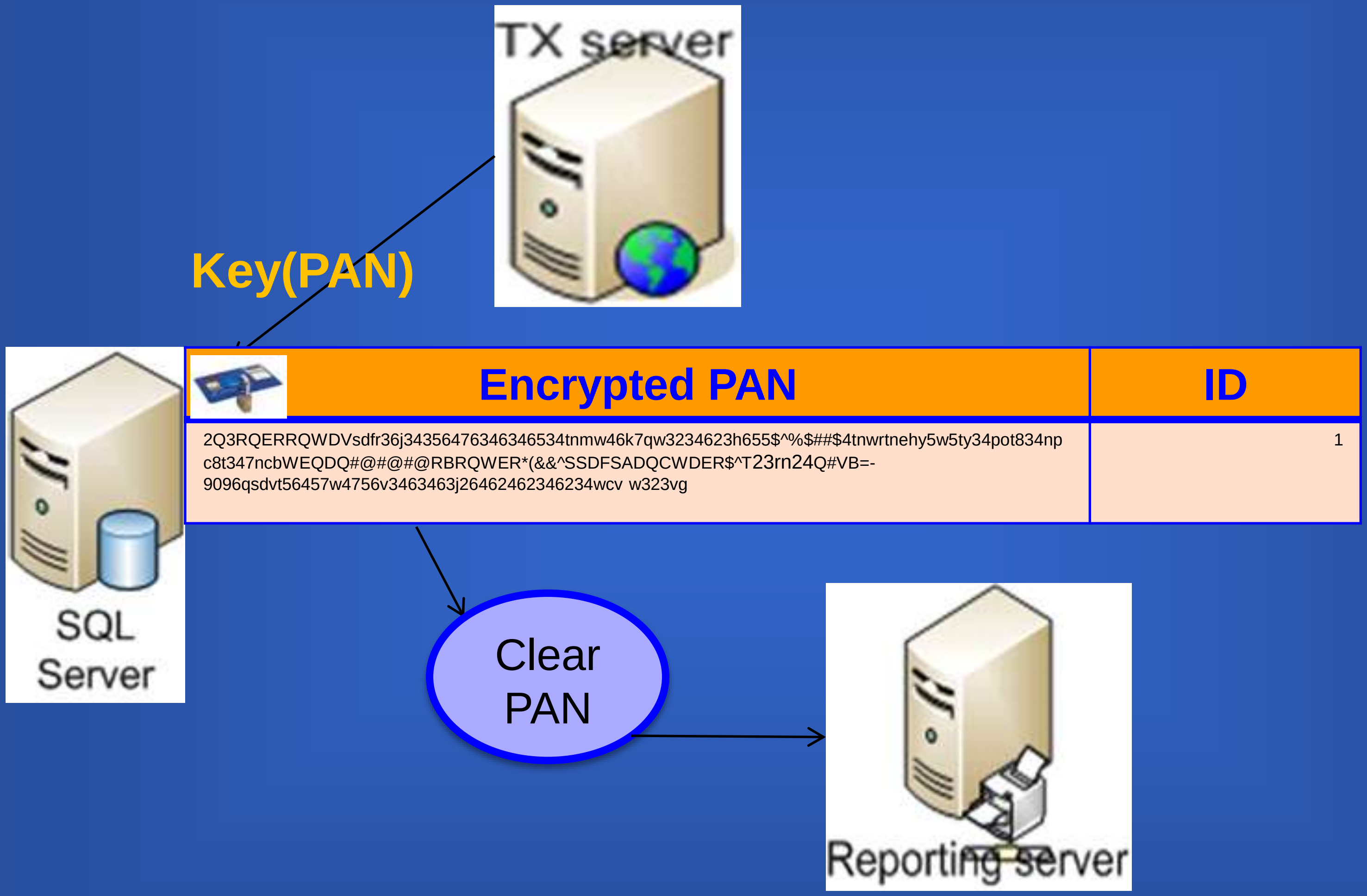
- Only one key
- Symmetric Encryption.
- Split keys:
  - DB
  - FS

- Complex – process to change key .

Case Study #1 - generating & using EK

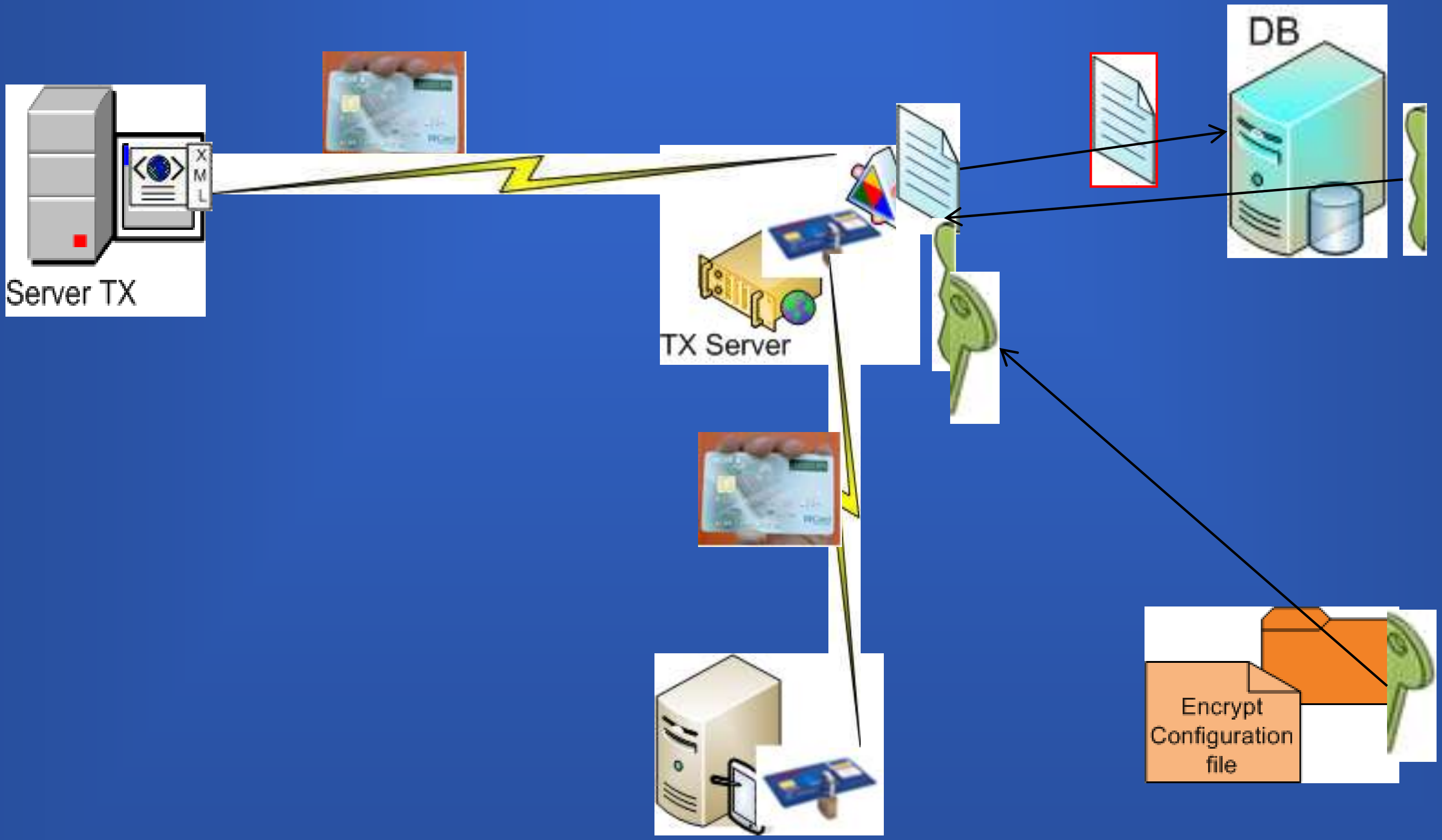


Case Study #1 - Payment Data TBL



Encrypted PAN	ID
2Q3RQERRQWDVsdfr36j34356476346346534tnmw46k7qw3234623h655$^%$##$4tnwrtnehy5w5ty34pot834npc8t347ncbWEQDQ#@#@#@RBRQWER*(&&^SSDFSADQCWDER$^T23rn24Q#VB=-9096qsdvt56457w4756v3463463j26462462346234wcv w323vg	1

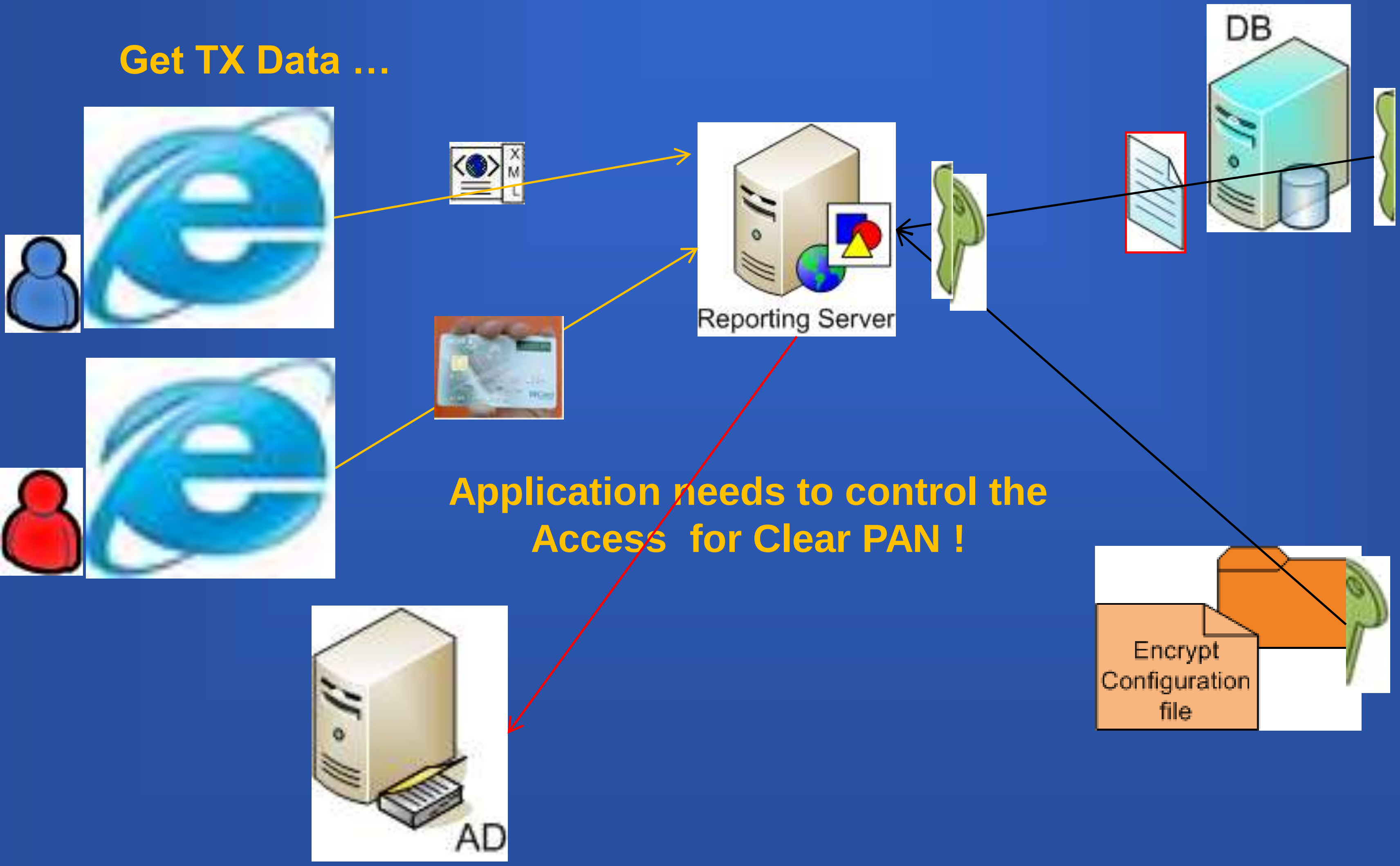
Case Study #1 - Transactions process



Credit Card Company

Case Study #1 - Reporting process

Get TX Data …



Application needs to control the Access for Clear PAN !

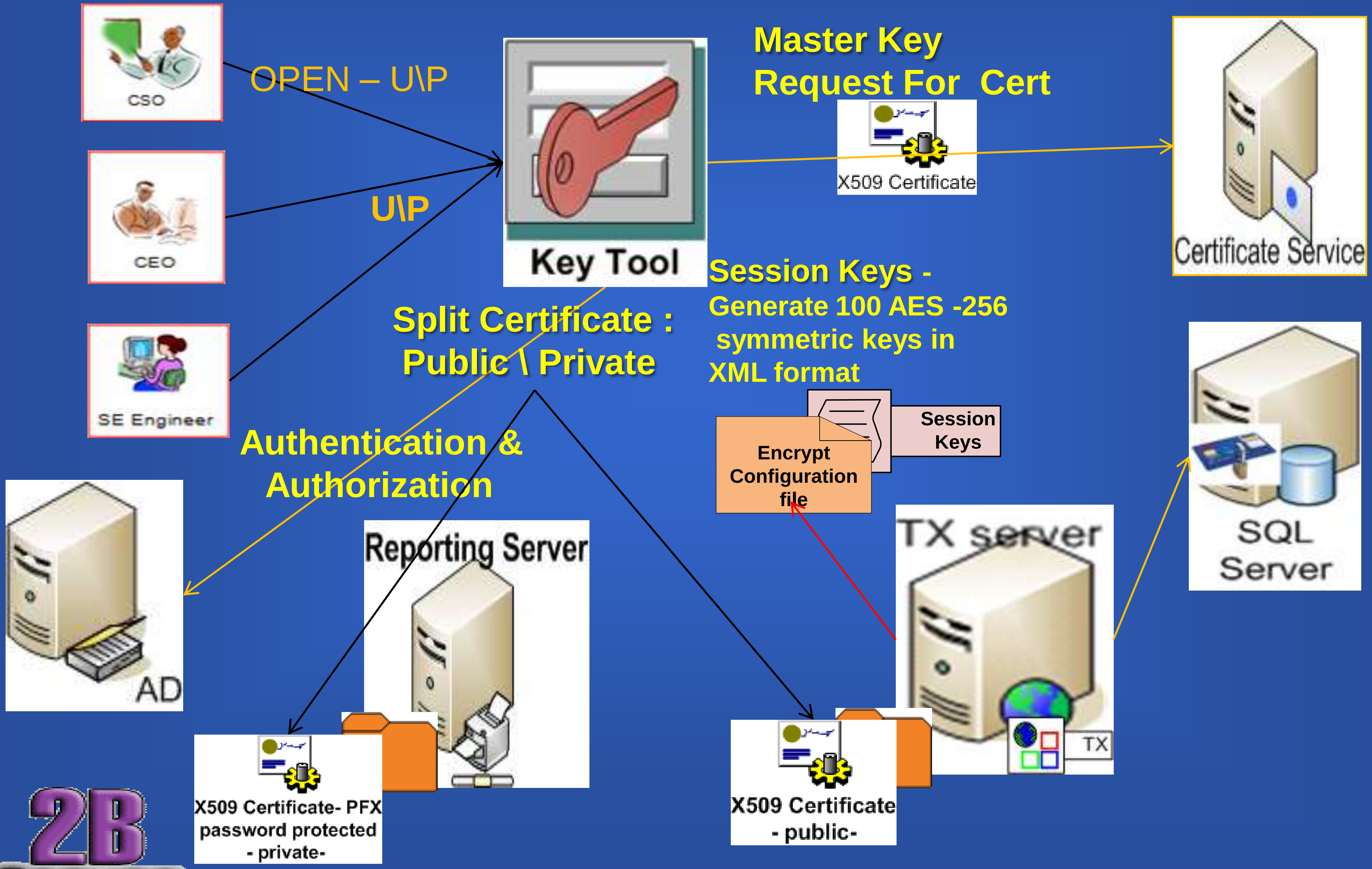
Key Management - Case Study #2

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

Advantages:

- More Secure – strong encryption.
- **Split knowledge and establishment of dual control**.
- Advantages:
  - process to change key.
  - Add new application.

Case Study #2 – Master & Session Keys



CSO

CEO

SE Engineer

OPEN – U\P

U\P

Key Tool

Master Key

Request For Cert

X509 Certificate

Certificate Service

Session Keys -

Generate 100 AES -256 symmetric keys in XML format

Split Certificate : Public \ Private

Session Keys

Encrypt Configuration file

Authentication & Authorization

AD

Reporting Server

TX server

TX

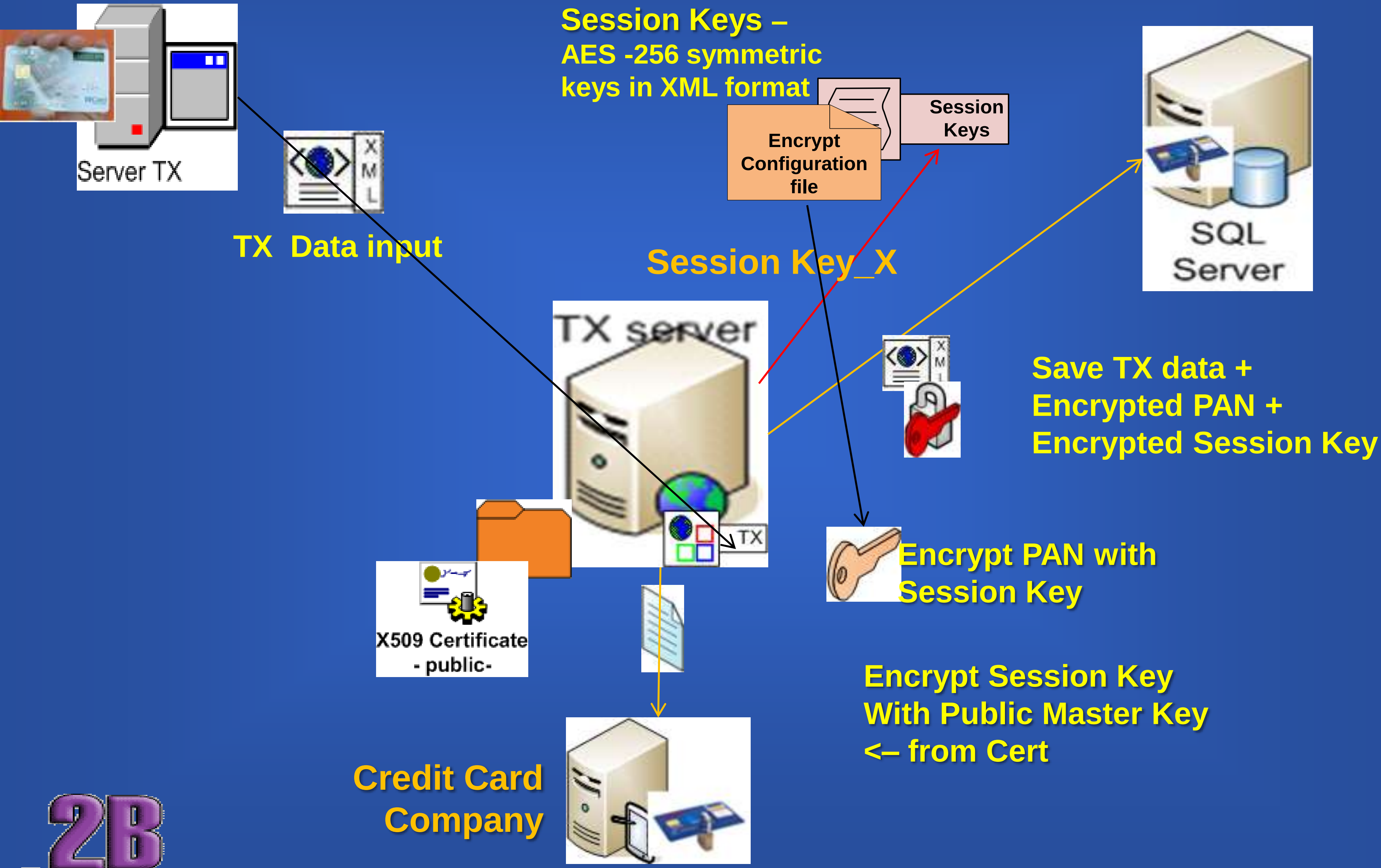
SQL Server

X509 Certificate- PFX password protected - private-

X509 Certificate - public-

© BY. <Yaron Hakon/> 2BSecure.

Case Study #2– Master & Session Keys



Session Keys –
AES -256 symmetric
keys in XML format

Encrypt Configuration file

Session Keys

TX Data input

Session Key_X

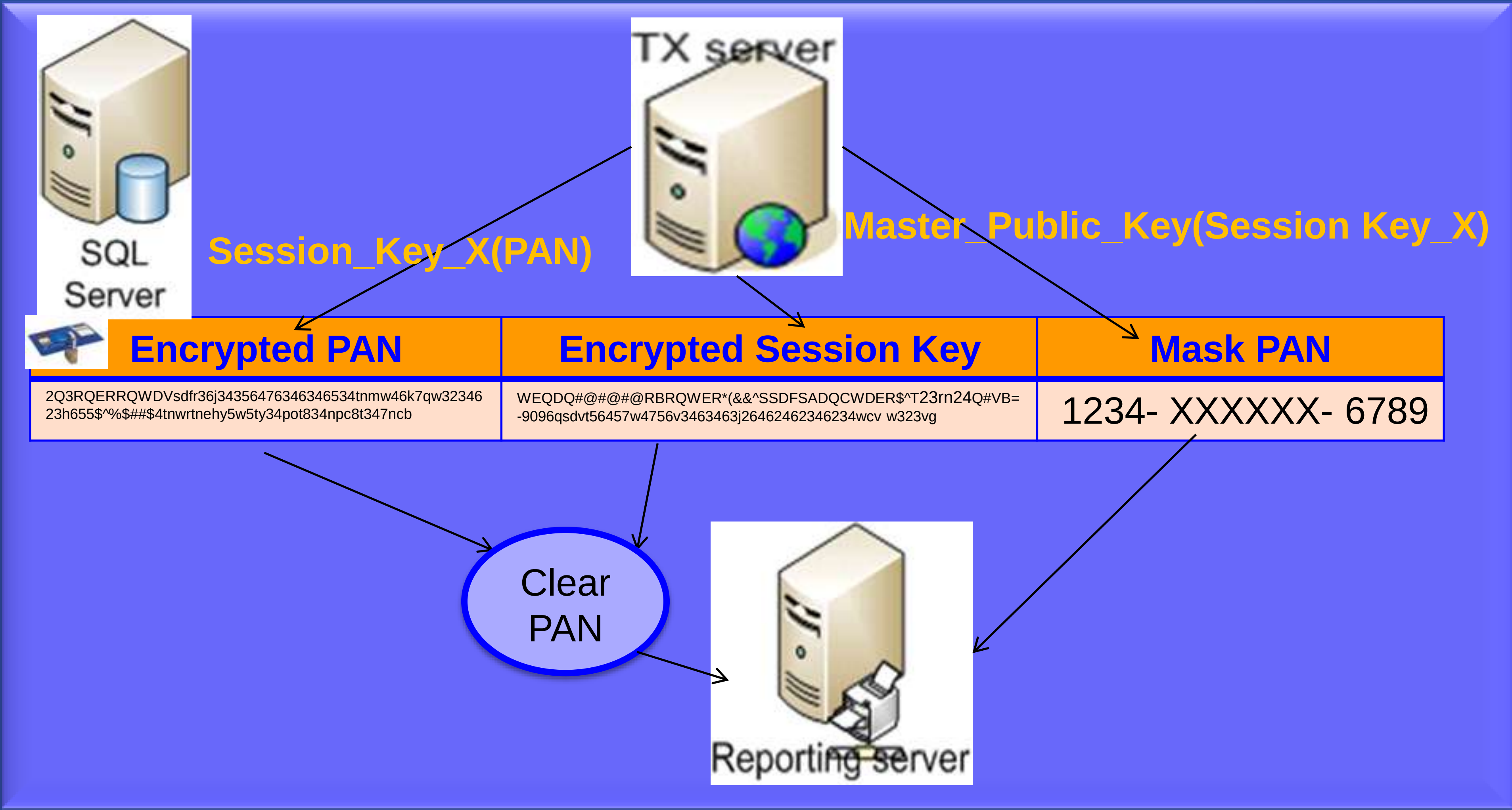
Save TX data +
Encrypted PAN +
Encrypted Session Key

Encrypt PAN with
Session Key

Encrypt Session Key
With Public Master Key
<– from Cert

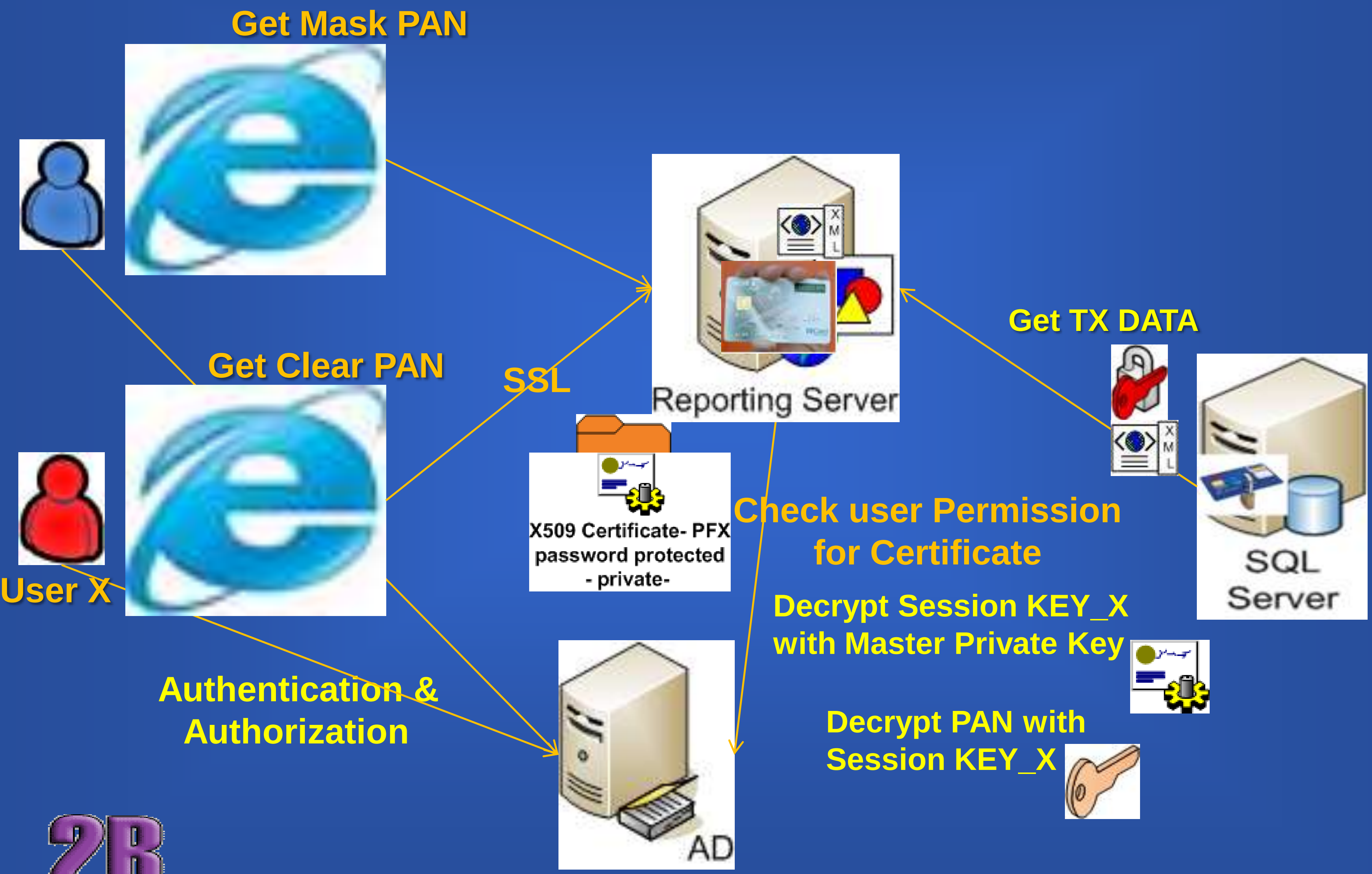
Credit Card
Company

Case Study #2 - Payment Data TBL



Encrypted PAN	Encrypted Session Key	Mask PAN
2Q3RQERRQWDVsdfr36j34356476346346534tnmw46k7qw32346 23h655$^%$##$4tnwrtnehy5w5ty34pot834npc8t347ncb	WEQDQ#@#@#@RBRQWER*(&&^SSDFSADQCWDER$^T23rn24Q#VB= -9096qsdvt56457w4756v3463463j26462462346234wcv w323vg	1234- XXXXXX- 6789

Case Study #2 - Reporting Service - Decryption



Check user Permission for Certificate

Decrypt Session KEY_X with Master Private Key

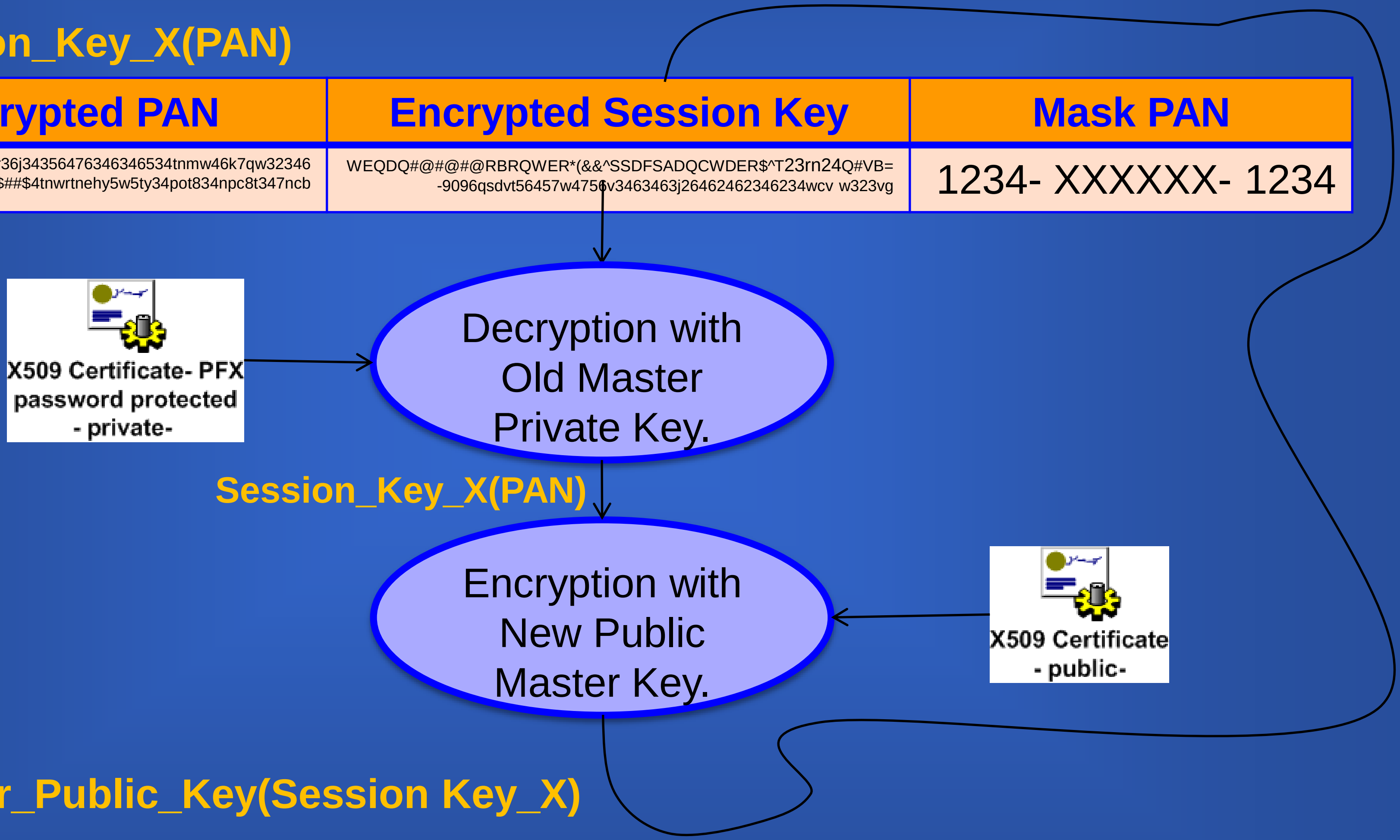
Decrypt PAN with Session KEY_X

Authentication & Authorization

Case Study #2 - Changing the Master Key

Session_Key_X(PAN)

Encrypted PAN	Encrypted Session Key	Mask PAN
2Q3RQERRQWDVsdfr36j34356476346346534tnmw46k7qw32346 23h655$^%$##$4tnwrtnehy5w5ty34pot834npc8t347ncb	WEQDQ#@#@#@RBRQWER*(&&^SSDFSADQCWDER$^T23rn24Q#VB= -9096qsdvt56457w4756v3463463j26462462346234wcv w323vg	1234- XXXXXX- 1234



X509 Certificate- PFX password protected - private-

Decryption with Old Master Private Key.

Session_Key_X(PAN)

Encryption with New Public Master Key.

X509 Certificate - public-

Master_Public_Key(Session Key_X)

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

- PCI requirements - https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml
- PCI Explain - http://www.rapid7.com/pci/pci-dss.jsp
- .NET encryption: AES
  - http://msdn.microsoft.com/en-us/library/system.security.cryptography.aes.aspx
  - http://msdn.microsoft.com/en-us/magazine/cc164055.aspx
- .NET DPAPI
  - http://msdn.microsoft.com/en-us/library/ms995355.aspx
- .NET RNGCryptoServiceProvider
  - http://msdn.microsoft.com/en-us/library/system.security.cryptography.rngcryptoserviceprovider.aspx

Visit my sites at:

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

www.2BSecure.co.il