

Cryptography Key Management

**ISACA Chapter meeting
27 June 2009
Mumbai**

Discussion Flow

§ Introduction to Gloqal	Rajesh C
§ Appreciating the situation	All of us
§ Global trends (fraud)	Narayanan K
§ Cryptography	Narayanan K
§ Cryptography Key Management	Narayanan K
§ Recommended controls (standards)	Narayanan K
§ Common errors	Narayanan K
§ Key Management Life Cycle	Narayanan K
§ Analyzing the situation	All of us
§ Way forward	All of us

Introduction to Gloqal

Enterprise Architecture Consulting

Domain IT & Process Consulting

BFSI

Consumer Products

Credit Cards – Loyalty Mgmt, PCI

MES, Process Control Systems

Investmt Banking – Trading Platforms

ERP, SCM, R&D

Productivity
Consulting

Infra
Consulting

Info & IT
Security

App
Consulting

Productivity Metrics &
Enforcement

Architecture & Design

Strategic Security
Assessment

Arch Efficiency Sols
(ATAM)

Application
Rationalization

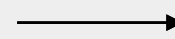
Bespoke Security
Consulting

Based out of Cincinnati, OH, USA with offices in Hyderabad, India

Customers: Global Fortune 50 Consumer Products Company, State of Ohio (USA)

Our daily challenge...

§ A faceless bank??



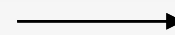
TBI (Test Bank Int'l)

ASSUMPTIONS

§ A credit card user base



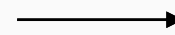
§ Account range



§ Average credit limit



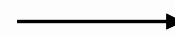
§ Daily transaction load



§ Current Fraud level



§ **Max Fraud Potential**



Daily transaction load

INR

million

Current fraud level

INR

million (DAILY)

Numbers

Recent threats - Banking

§ ATM attacks Apr '09

- €30 K withdrawn from an ATM between 23:00 & 07:00 (following day)
- 16 cards confiscated by the ATM
- Customer's account not impacted
- ATM physically compromised

Courtesy: Confidential sources

§ Decimalization table attacks

- Determine what digits are in the PIN (in an incorrect order)
- Determine the order of the digits
- Takes ~ 13.5 attempts to "guess" a PIN from the PAN (card number)

Courtesy: Paper by Graham Steel, Univ of Scotland

Vulnerable plastic

§ 200 million credit cards compromised since 2006

(courtesy Privacy Rights Clearing House)

§ Hundreds of millions more – vulnerable

§ Only a max of 7 of 16 digits in a card number is unique (and they are in incremental values)

§ Possible 1 – 10 million cards in an account range; protected by a single cryptography key

§ An attacker can compromise all 10 million cards or compromise the cryptography key

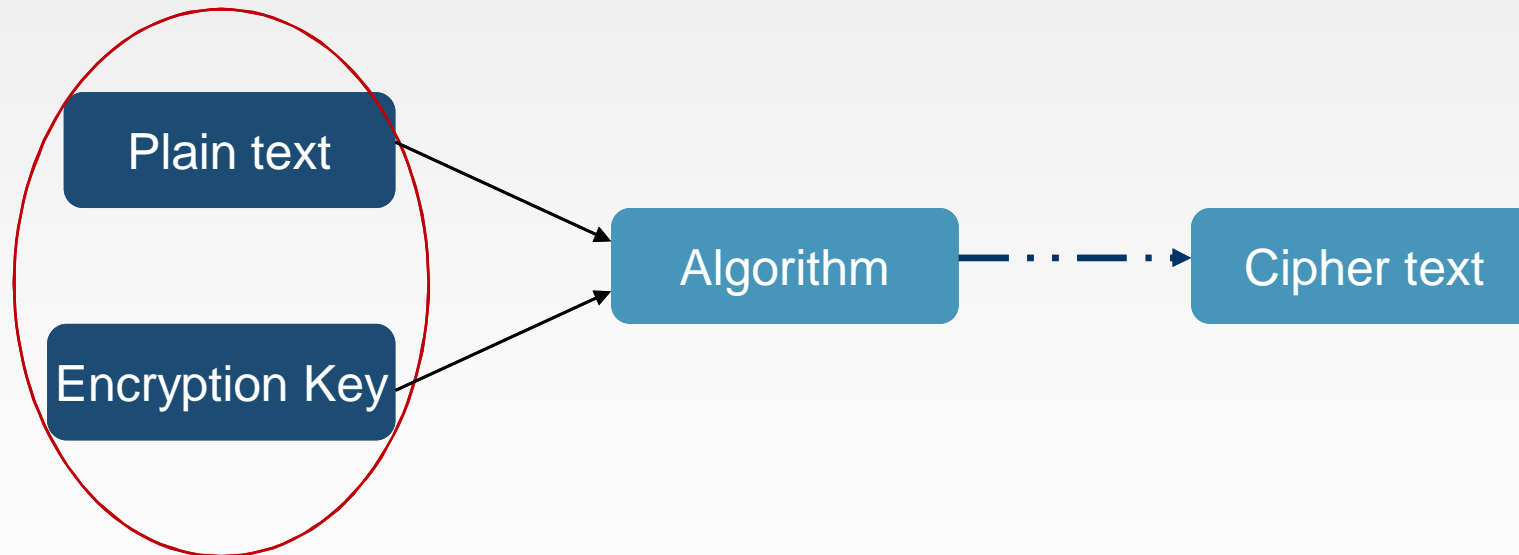
Drip through holes in Cryptography Key Management processes

Cryptography

- § The process of scrambling data to maintain integrity and confidentiality
- § Two critical assumptions in cryptography:
 - The algorithm is known publicly
 - The cipher text is available to the attacker
- § Facts about cryptography
 - Security is enhanced by using one way cryptography algorithms
 - Given a set of records (cipher text), using brute force cryptanalysis, an attacker can guess the plain text

Cryptography Key Management

§ Given that the algorithm and cipher text is available to the attacker



§ The Plain text is safe only if the encryption key is secure

§ In addition to sufficiently secure long keys (key length), efficient controls are required

ISO 11568 “Principles of key management”

1. Keys shall only exist in those forms permitted by ISO 11568
2. No one person shall have the capability to access or ascertain any plaintext secret key.
3. Systems shall prevent the disclosure of any secret key that has been or will be used to protect any data.
4. Secret keys shall be generated using a process such that it is not possible to predict any resultant value or to determine that certain values are more probable than others from the total set of all the possible values.
5. Systems should detect the attempted disclosure of any secret key and the attempted use of a secret key for other than its intended purpose.
6. Systems shall prevent or detect the use of a secret key, or portion of that key, for other than its intended purpose, and the accidental or unauthorised modification, use, substitution, deletion or insertion of any key.

Courtesy: Mr. Andrew Moore, ISACA UK Northern Chapter
Full ppt available [HERE](#)

ISO 11568 “Principles of key management” (continued)

7. A key shall be replaced with a new key within the time deemed feasible to determine the old key.
8. A key shall be replaced with a new key within the time deemed feasible to perform a successful dictionary attack on the data enciphered under the old key.
9. A key shall cease to be used when its compromise is known or suspected.
10. The compromise of a key shared among one group of parties shall not compromise keys shared among any other group of parties.
11. A compromised key shall not provide any information to enable the determination of its replacement.
12. A key shall only be loaded into a device when it may be reasonably assured that the device is secure and has not been subjected to unauthorised modification or substitution.

Courtesy: Mr. Andrew Moore, ISACA UK Northern Chapter
Full ppt available [HERE](#)

Cryptography Key Management – common errors

§ Segregation of duties

- Teams that use the keys -- handle them



§ Split access

- Keys are split into multiple components
- All components are stored in the same place OR
- All components are handled by one person



§ Integration with Fraud Management

- Fraud detection continues at card level



§ Detection of key compromise

- No steps to detect possible key compromise
- Thus no steps to respond to such situations



But my process is in good shape...??

People
Movement

Long Term
Sigma shift

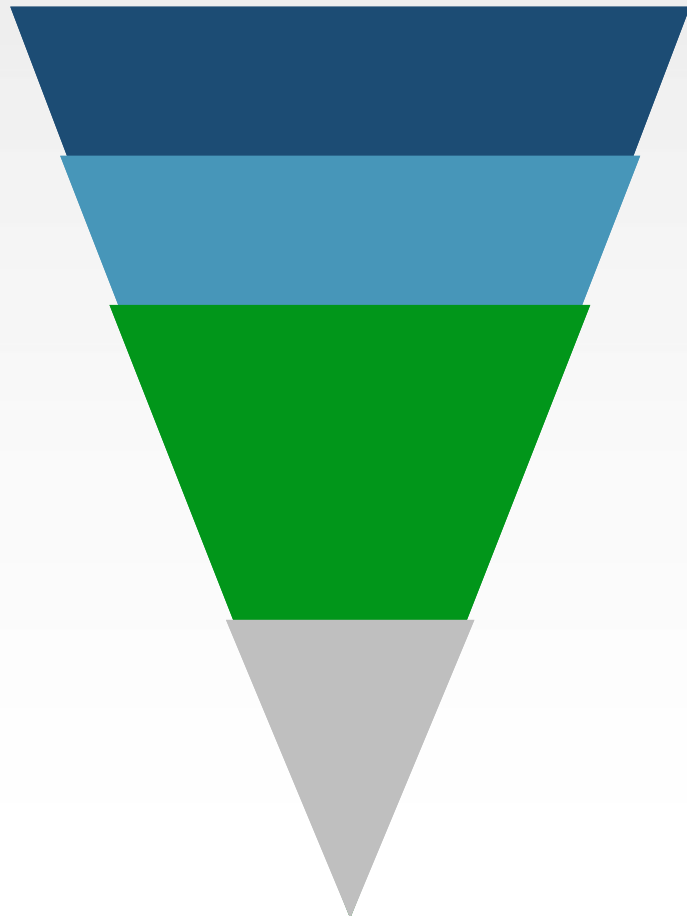
Ever changing
Compliance requirements

Information Security
Implementation in SILOS

Solving the problem
HERE & NOW

Distinct disconnect between Business Drivers & Information Security

Way Forward



Implement Point Technology Solutions

Redesign Business Processes

**Transition Roadmap
Maturity Assessment**

**Business – InfoSec
alignment**

Way Forward

- § Revisit Information Security architecture alignment with business drivers
- Enablers for business growth
 - Solutions for risk management (including fraud / chargebacks)
 - Visionary approach – future proofing

Enterprise Architecture Approach



Thanks

Contact:

Narayanan Krishnan **+91 97035 11163**
narayanank@gloqalinc.com

Rajesh Chundi **+91 96522 24259**
chundirr@gloqalinc.com

Annexure

Appreciating the situation – my assumptions

§ Let us create a fictitious bank → TBI (Test Bank Int'l)

ASSUMPTIONS

§ Let us assume a credit card base → 1 million

§ Account range → 1

§ Average credit limit → INR 100,000

§ Daily transaction load → 0.5 % of total credit limit

§ Current Fraud level → 8% of daily transactions

§ **Max Fraud Potential** → **Daily transaction load**

Daily transaction load INR 500 million

Current fraud level INR 40 million (DAILY)

[Back](#)

Cryptography Key Management - standards

§ Choice of encryption algorithm

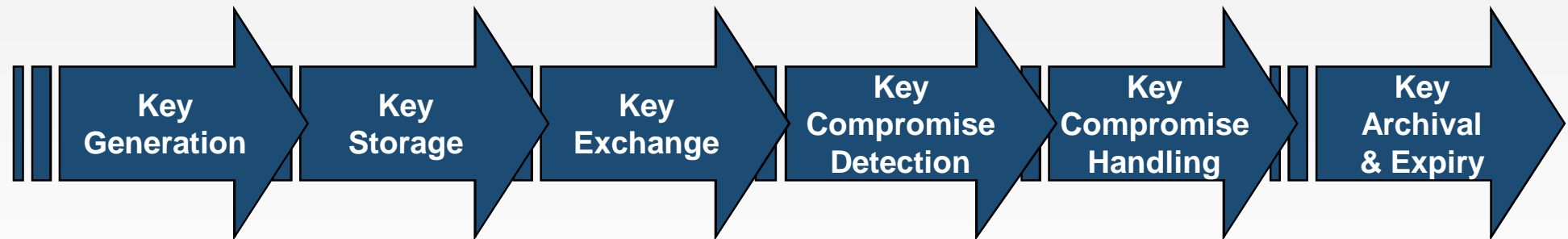
- Symmetric Key Encryption: Increasing key length by 1 byte increases complexity by 2 X; against asymmetric (1.12 X)

§ Standards

- ISO 11568 (specific for banks) – list of recommended controls
- ISO 11770 – Cryptography Key Management LifeCycle
- PCI DSS (TG 3) – list of minimum controls
- ISO 9564 – recommended encryption and key management controls

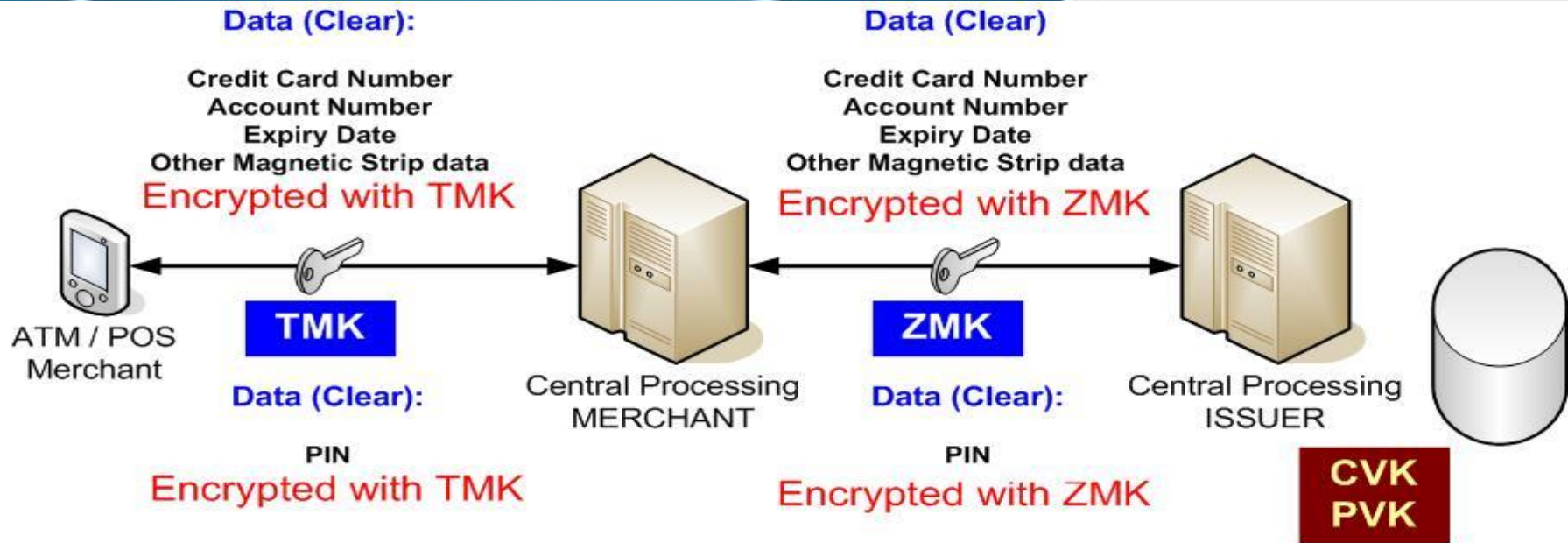
§ Most controls are implemented, but due to “age”, errors creep in

Cryptography Key Management – Life Cycle



Courtesy: ISO 11770

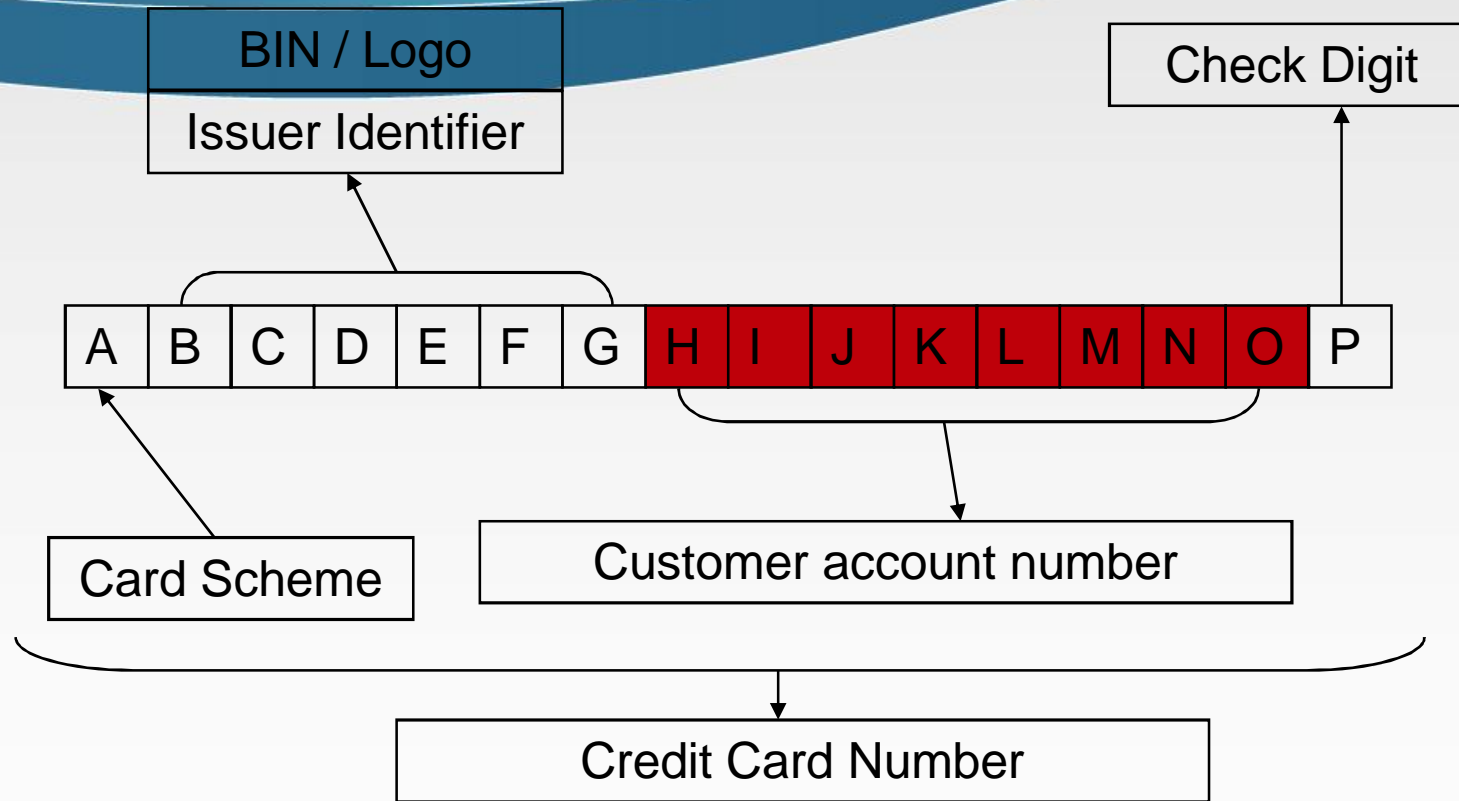
Introduction 4 – ATM to Issuer and back



Legend:

TMK: Terminal Master Key
ZMK: Zone Master Key
CVK: Card Verification Key
PVK: PIN Verification Key

Anatomy of a credit card



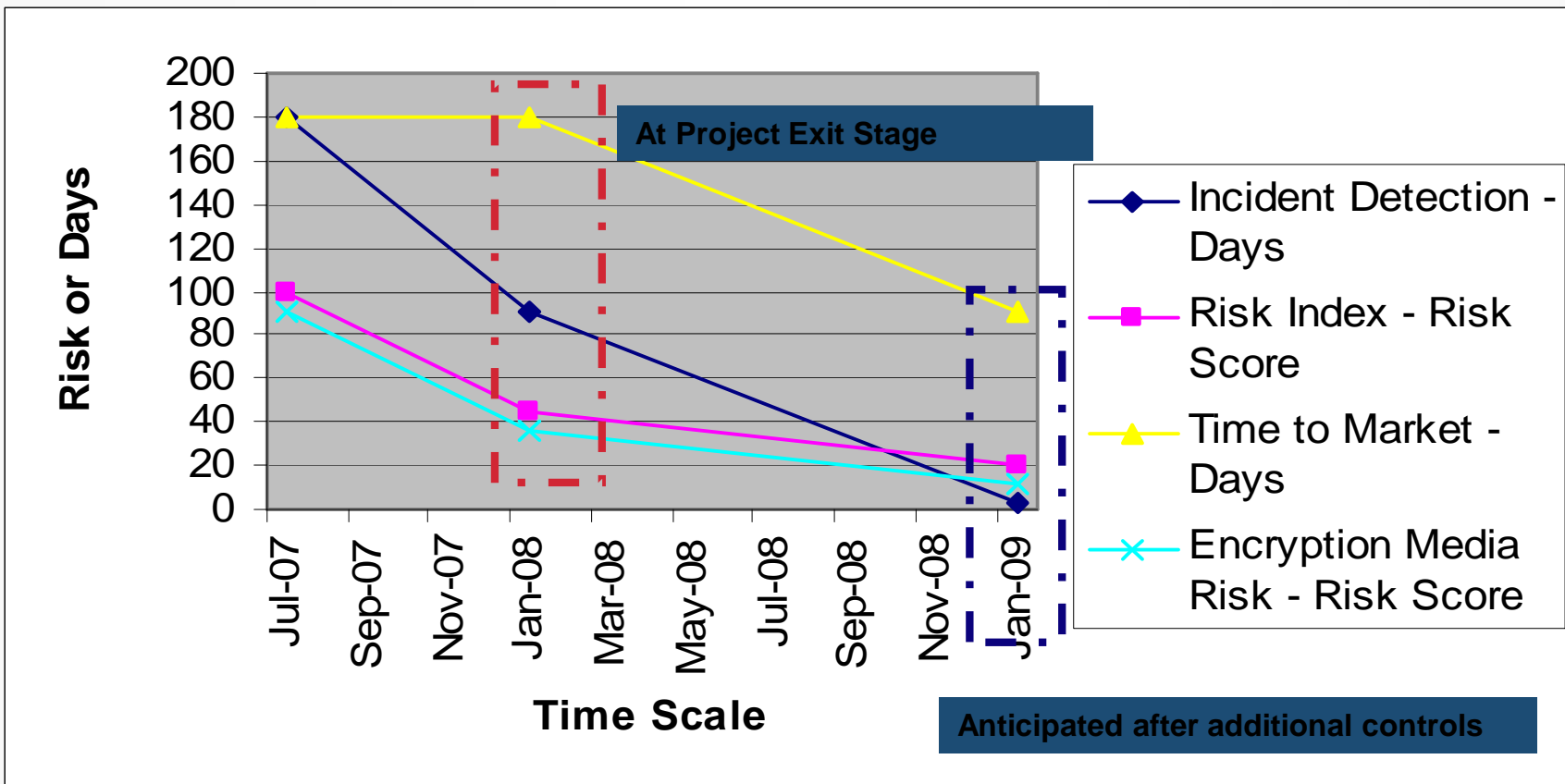
Credit Card Number  Card Verification Key  Card Verification Value

Credit Card Number  PIN Verification Key  PIN

Delivered Impact – recent project

§ Risk Reduction – US\$ 1 billion per group

§ Cash Flow impact of US\$ 88 million



Appreciating the situation – questions???

- § Percent of CNP fraud v/s other forms of fraud
- § Value of CNP fraud v/s other forms of fraud
- § Trend of fraud (amount, merchant, product)
- § Donations to NGO's; non profit organizations
- § Do our cryptography keys change (refresh cycle) regularly?

- § Audit of cryptographic keys & their management process