Certified Card Payment Systems Professional (CCPSP)™

Program Courseware

MVL Consulting Private Limited
#17, Laxman Villa Condominium, Paud Road, Pune 411038, India
Email: info@mvlco.com Website : www.mvlco.com

CIPSP™
CPPS™
CCPSP™
CPME™

2018

MVLCO

Let our internationally acclaimed Payment Domain Certifications elevate your career!

Register today!

Payments are an inherent part of our daily life. Strong and robust payment systems are a key to financial stability and economic growth. With continuous evolution and rapid progress, payment industry offers great opportunities. Entry of non-bank players and technology innovations are adding more zing to payments.

It is very important for banks, technology companies, players in payment industry as well as professionals working with them to have a thorough knowledge of end-to-end processes, business / career opportunities, regulation and developments in payments.

Participants from many central banks, clearing houses, IT companies, and banks from USA, Europe, Asia, Africa and Middle-east have already been certified.

Get certified!
Stay ahead of the competition!

- Certified International Payment Systems Professional
- Certified Payment Processing Specialist
- Certified Card Payment Systems Professional
- Certified Payment Messaging Expert

Four Aces Payment Domain Certifications

Training programs for all the certifications are available in classroom mode, live virtual classroom (webinar) mode and recorded training mode.

Special Offer

Contact us for special offers on course combinations.

www.mvlco.com

Recorded Webinars

AVAILABLE

All our training programs are also available in-house. To arrange an in-house program please **contact us:**

+91-9764835350
or email
info@mvlco.com

2018

Register today!

MVLCO

Certified International Payment Systems Professional (CIPSP)™

CIPSP certification will help you in enhancing your skills in International Payment Systems.

Get certified! Stay ahead of the competition!

MVLCO offers a four full days comprehensive CIPSP certification program extensively focused on International Payment Systems. The course covers important payments systems in countries i.e. USA, Europe (SEPA), Canada, Hong Kong, China and India with detailed understanding of each of the payment systems including RTGS, Hybrid Systems and using cryptocurrencies like Bitcoin to make payments.

The CIPSP program emphasizes on active participation from delegates and includes exercises and case studies.

When you complete CIPSP, you will have complete understanding of :

- What are payment and settlement systems
- What are the risks in payment systems
- How paper based payment systems operate
- How electronic payment systems operate
- How cryptocurrencies are used to make payments
- How instant payments like IMPS or NPP are made
- How international payments are made
- SWIFT and other messaging systems for payments
- Overview of card and mobile payments
- AML/CFT/FATCA regulation

LIVE VIRTUAL CLASSROOM

Certification training is available in (a) live classroom mode (b) live virtual classroom mode (c) webinar mode (d) Studio recordings mode and (e) recorded classroom mode.

Certified International Payment Systems Professional (CIPSP)

MVLCO

Payments are an inherent part of our daily life. Strong and robust payment systems are a key to financial stability and economic growth.

With continuous evolution and rapid progress, payment industry offers great opportunities. Entry of non-bank players and technology innovations are adding more zing to payments.

It is very important for banks, technology companies, players in payment industry as well as professionals working with them to have a thorough knowledge of end-to-end processes, business / career opportunities, regulation and developments in payments.

Our payment certification programs will equip you to gain thorough knowledge about wholesale and retail and payment systems of all types. Our payment certification programs are acknowledged and accepted by central banks, global commercial banks, clearing houses, IT and software companies and are used by them for skill enhancement of payment professionals within their organizations.

Participants from many Central Banks, Multinational Commercial Banks, Clearing Houses and software/IT companies from Asia, Americas, Europe, Africa and Middle-east have already been certified.

International and domestic payments are one of the most happening domain areas in banking and finance. Large opportunities exist for **Payment Professionals** in banks and IT/ Software industry.

Course contents

Introduction

- Importance of payment and settlement system
- Three key elements : Message, Clearing/Netting and Settlement
- Paper to electronic payments – check truncation/conversion, Check 21, Remote deposit capture
- Payment processing
  - Paper to paper
  - Paper to electronic
  - Electronic to electronic
  - Electronic to paper – Cheque Processing service
- Using Cryptocurrencies to make payment e.g. Bitcoin
- Mobile payments

Why does a bank make payments

- Own account transactions including position maintenance and cover operations
- Customer transactions

Risks in Payment Systems :

- Herstatt risk, Credit Risk,
- Liquidity Risk,
- Systemic Risk
- Operational Risk.

Risk mitigation techniques

- Carefully chosen members
- Novation, Central counterparty system
- Loss sharing arrangements,
- Collateral
- Other mitigation techniques

Relationship structures

- Correspondent banking
- Bilateral clearing arrangements
- Network managed banking

Payment types

- Book payments
- Local payments
- Domestic payments
- Cross border payments,

Payments systems

- Real Time Gross Settlement (RTGS) ,
- Real Time Net Settlement (US CHIPS and Canadian LVTS)
- Net Settlement,
- Hybrid settlement (STEP2)
- Continuous Linked Settlement (CLS)

FSI ACADEMY

www.mvlco.com

Certified International Payment Systems Professional (CIPSP)

MVLCO

Course contents (Continued)

Regional payments systems

- USA payment systems : Fedwire, CHIPS, NSS, ACH
- SEPA payment systems : TARGET2, STEP 2 (SCT/SDD) PE-ACH
- China payment systems : CDFCPS/CIPS
- Hong Kong payment systems : CHATS
- Canadian payment systems : LVTS
- Indian payment systems : RTGS, NEFT, IMPS, UPI

Using cryptocurrencies for making payment

- Introduction to Cryptocurrencies e.g. Bitcoin
- Blockchain, Distributed Ledger Technology and Wallets
- Transaction processing and mining
- Pros and cons of Cryptocurrencies

Card and mobile payments overview

- Introduction to card payments and mobile payments
- Remote payments and proximity payments
- A brief overview of ISO 8583
- Transaction processing using cards and mobile for payments

Overview of SWIFT messaging : MT and MX messages

- Role of SWIFT in payment systems
- SWIFTnet Fin, Fileact, Interact, Browse
- SWIFT payment message processing – MT 1XX, MT 2XX, MT 9XX, MX PAIN/ PACS
- SWIFT Payment Messages examples
- SWIFT for corporates

Use of codes in payment systems

- Codes – IBAN, BBAN, BIC, BEI, UID, UPIC, ABA routing codes, IFSC .

Overview of foreign exchange from payments perspective

- Cash, TOM, Spot, Forwards
- Interbank transactions
- Merchant transactions
- Exchange rate determination and rate computation

Cash management products

- Concept of float
- Cash concentration, notional pooling and sweep
- Virtual account management (VAM)
- Controlled disbursements, positivepay, reverse positivepay
- ACH filter/ACH block
- Lockboxes

Impact of regulation

- Basel Committee on Systemically Important Payment and Settlement Systems
- FATF/OFAC compliance
- Wolfsberg Group compliances
- FATCA/GATCA compliance
- AML compliance

BFSI ACADEMY

www.mvlco.com

Certified International Payment Systems Professional (CIPSP)

MVLCO

Course modules

Module 1 : Basics of payment systems

Module 2 : Risks in payment systems

Module 3 : Introduction to RTGS /Hybrid payment systems

Module 4 : Introduction to SWIFT MT and MX messages

Module 5 : Fedwire RTGS in USA

Module 6 : CHIPS in USA

Module 7 : ACH and NSS operations in USA

Module 8 : Introduction to SEPA and TARGET2

Module 9 : SEPA SCT and SEPA SDD

Module 10 : China FCDPS, CIPS and HKMA CHATS

Module 11 : Large Value Transfer System, Canada

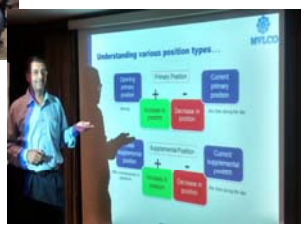
Module 12 : Continuous Linked Settlement System

Module 13 : Bitcoin and Cryptocurrencies

Module 14 : Card and Mobile payments

Module 15 : Cash management products

Module 16 : Anti-money laundering and other regulation



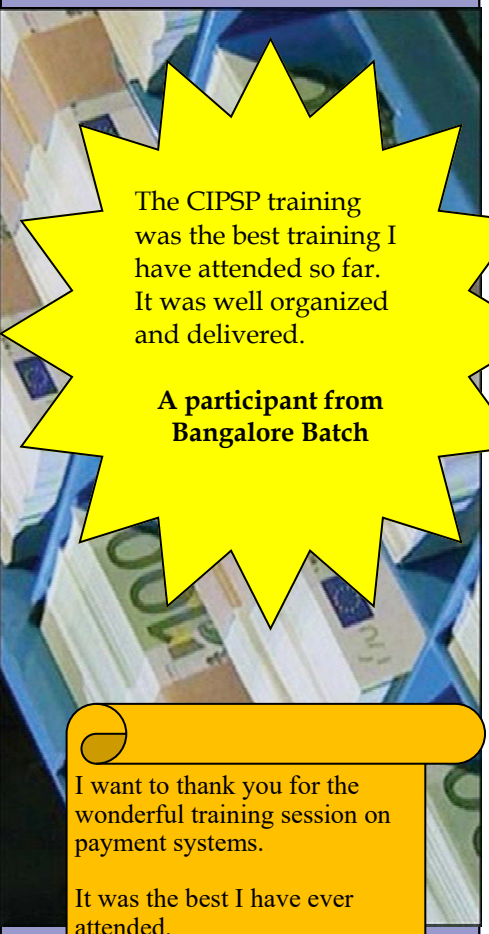
Get Certified ! Stay Ahead of the Competition !

BFSI ACADEMY

www.mvlco.com

Certified International Payment Systems Professional (CIPSP)

MVLCO



The CIPSP training was the best training I have attended so far. It was well organized and delivered.

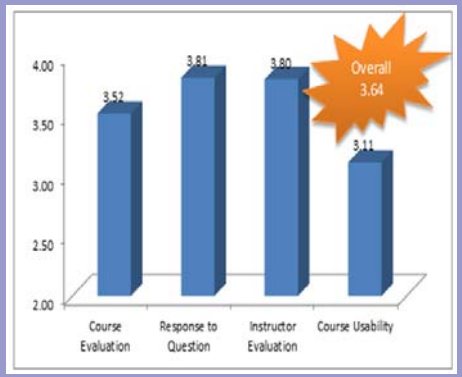
A participant from Bangalore Batch

I want to thank you for the wonderful training session on payment systems.

It was the best I have ever attended.

With the very meticulous collection of data / processes and supporting material, structured presentations, clear sequencing of the sessions, the efficiency of the training was as enjoyable as much as it was informative.

- Srikrishnan Jayaraman,
Consulting Practice Director
Oracle Bangalore



Program feedback from one of the largest global banks (Overall 3.64 out of 4.00)
CIPSP program conducted in-house is continuously receiving excellent response and feedbacks from multi-national banks and IT companies.

Participants speak:

The Program was so carefully designed, that every single second of time became very interesting, The way the trainer drove us through the program was just amazing, there was no confusion or bumps during the session.

: **Maheshkumar, Oracle**.

The program was very interesting and the trainer made it even more interesting. The basic were made strong first and then the advanced topics were taken. This made it easier for everyone. The trainer also had answers for any questions encountered.

: **Participant from National Payments Corporation of India (NPCI)**

The program touched upon all the concepts with respect to payments. Getting this much information from a single source is simply outstanding.

: **Saurabh Sharma, HSBC**.

Given the amount of knowledge being imparted, the trainer managed to engage us right through the 4 days and kept us completely glued to the course !

: **Sanjay Kumar, Oracle**

Very useful program. I had very limited exposure to banking. But I carry back with myself a lot of learning!

: **Akhil , Infosys**.

It is a very useful and well designed program . The flow is also excellent

: **Vaibhav Vaze, Barclays**.

Very insightful and interactive program !

: **Vivek Tiwari British Council**.

MVL Consulting Private Limited
#17, Laxman Villa Condominium, Near Jog Hospital, Paud Road, Pune 411038 India
Telefax: +91-20-25466154, +91-20-25422874 Mobile: +91-9764835350

BFSI ACADEMY

www.mvlco.com

Certified International Payment Systems Professional (CIPSP)

MVLCO

CIPSP @ Bangalore

CIPSP @ NPCI, Mumbai

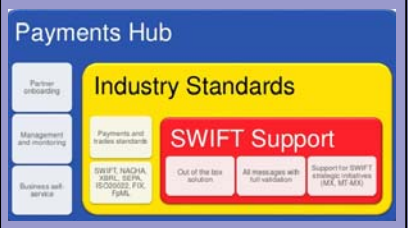
CIPSP Bangalore
More than 40 participants from Oracle, IBM, Wipro, Infosys, Congizant, LankaClear, RS Software and other reputed organisations attended the program.

CIPSP Pune
More than 20 participants from Barclays, Tieto, Oracle, IBM, and other reputed organisations attended the program.

MVL Consulting Private Limited
#17, Laxman Villa Condominium, Near Jog Hospital, Paud Road, Pune 411038 India
Telefax: +91-20-25466154, +91-20-25422874 Mobile: +91-9764835350

BFSI ACADEMY

www.mvlco.com



All our training programs are also available in-house. To arrange an in-house program please **contact us on** :

+91-9764835350 or email info@mvlco.com

2018

Register today!

MVLCO

Certified Payment Processing Specialist (CPPS)™

CPPS certification will help you in enhancing your skills in payment processing.

Get certified! Stay ahead of the competition!

Payments are an inherent part of our daily life. With Continuous evolution and rapid progress, payment industry offers great opportunities. Entry of non-bank players and technology innovations are adding more zing to payments. It very important for banks, technology companies, players in payment industry as well as professionals working with them to have a thorough knowledge of end-to-end processes, opportunities and developments in payments.

MVLCO offers a four full days comprehensive CPPS certification program extensively focused on processing wholesale and retail payments.

When you complete CPPS, you will have complete understanding of :

- How wholesale and retail payments are processed
- Structure of SWIFT MT/MX payment messages
- How payment engines and payment hubs function
- Exceptions, investigations, rejects and returns handling
- Frauds in payments / Payment analytics
- Current and future trends in payments

LIVE VIRTUAL CLASSROOM

Certification training is available in (a) live classroom mode (b) live virtual classroom mode (c) webinar mode (d) Studio recordings mode and (e) recorded classroom mode.

Certified Payment Processing Specialist (CPPS)™

MVLCO

Most of the global banks have completely automated their payment process from end-to-end.

These banks use various software applications from the point where corporate and retail customers create the payment, till the payment is released to beneficiary's bank in a straight through processing (STP) mode.

Such STP process requires software application for payment creation, for handling payment messages in standardized formats such at SWIFT or ISO20022, use of payment engines for decision making, integration with anti-fraud and AML/CFT engines, and many more such applications.

This course helps you understand

Why should you attend:
International and domestic payments are one of the most happening domain areas in banking and finance. Large opportunities exist for **Payment Professionals** in banks and IT/Software industry. After this certification you would have a cutting edge over others !

Course contents

Introduction

- Importance of payment systems
- Broad objectives and components of payment system
- Three key elements : Message, Clearing/Netting and Settlement
- Electronic Payment Systems viz. RTGS, Hybrids and Card Payments
- Payment transactions : Bank to Bank, Bank-to-Customer

Payment Messaging :

- Messaging methods i.e. internet, mobile, SWIFT etc.
- SWIFT/euroSIC/EDIFACT/proprietary messages
- Understanding SWIFT MT/MX message structure
- SWIFT MT Messages for payments i.e. 1XX, 2XX and 9XX
- SWIFT MX messages for payments i.e. PAIN, PACS and CAMT
- Message conversion and message processing, message repair

Payment Exceptions and Investigations

- Exceptions : request to cancel/request to modify
- Exceptions : Unable to apply
- Exceptions : Claim non-receipt
- Investigation : Resolution
- Investigation : Notification of case assignment
- Investigation : Duplicate/Request for duplicate
- Investigation : Rejection
- Investigation : Case status report request/report
- Investigation : Debit authorization request/response
- Use of software/applications to automate exceptions/investigations

Payment Rejects and Returns

- Understanding rejects and returns
- Understanding SWIFT reject/return guidelines
- Using SWIFT MT/MX messages for reject and return

Payment Engines. Payment Hubs and Straight Through Processing (STP)

- Components of payment engine/payment hub
- How payment engines/payment hubs function
- Payment processing using payment engines / payment hubs
- Payment accounting and transaction reconciliation
- Liquidity and queue management

Payment Accounting and Funds Management

- Payment accounting : Settlement Accounts, Nostro/Nostro Mirrors
- Payment transactions reconciliation

Frauds in Payments

- Types of frauds and fraud prevention

Payment Analytics

- Payment KPI/KRI and data analytics

Current and future trends in payments

BFSI ACADEMY

www.mvlco.com

Certified Payment Processing Specialist (CPPS)™

MVLCO

The course covers understanding of SWIFT MT/MX (ISO20022) messages used for payments, usage of payment engines to process payment transactions, straight through payment processing, treatment of rejects and returns, payment exceptions and investigations, and frauds in payments.

The CPPS program emphasizes on active participation from delegates and includes exercises and case studies. A certification test is conducted at the end of the program.

Course modules:

Module 1 : Basics of payment systems

Module 2 : Basics of paper payments

Module 3 : Electronic payment messaging

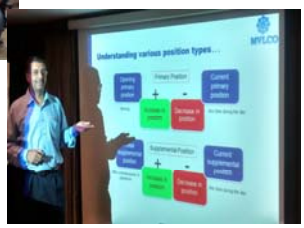
- SWIFT MT/ISO20022

Module 4 : Customer channels for electronic payments

Module 5 : Payment engine, payment hub and STP

Module 6 : Frauds in payments and payment analytics

Module 7 : Current and future trends in payment



Get Certified ! Stay Ahead of the Competition !

FSI ACADEMY

www.mvlco.com

2018

MVLCO

Certified Payment Messaging Expert (CPME)

CPME certification will enhance your knowledge and skills in structured electronic messages used in Payment Systems.

Get certified! Stay ahead of the competition!

MVLCO offers a four full days comprehensive CPME certification program extensively focused on messages and messaging standards used in payment systems. The course covers important messages formats e.g. SWIFT MT/MX , ISO 20022 , Fedwire and CHIPS messages used in payments systems.

The course covers understanding important message types at field/message component level. The PME program emphasizes on active participation from delegates and includes exercises and case studies.

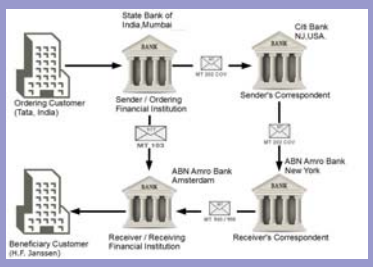
When you complete CPME, you will :

- Understand importance of messages in payment systems
- Gain knowledge about SWIFT MT messages for payments e.g. MT1XX, MT2XX and MT9XX series
- How ISO20022/SWIFT MX messages e.g. PAIN, PACS, CAMT are used for payments.
- Get an overview of Fedwire, CHIPS and ACH payment messages used in USA
- Understand end-to-end payment process using SWIFT MT and SWIFT MX / ISO 20022 messaging standards

Register today!

MT103 fields

Field	Field Name
:20	Transaction Reference Number
:23B	Bank Operation Code
:32A	Value Date / Currency / Interbank Settled
:33B	Currency / Original Ordered Amount
:50A, F or K	Ordering Customer (Payer)
:52A or D	Ordering Institution (Payer's Bank)
:53A, B or D	Sender's Correspondent (Bank)
:54A, B or D	Receiver's Correspondent (Bank)
:56A, C or D	Intermediary (Bank)
:57A, B, C or D	Account with Institution (Beneficiary's Bank)
:59 or 59A	Beneficiary
:70	Remittance Information (Payment Reference)
:71A	Details of Charges (BEN / OUR / SHA)
:72	Sender to Receiver Information
:77B	Regulatory Reporting



BFSI ACADEMY

BFSI Academy is the training division of MVL Consulting Private Limited.

Visit MVLCO at www.mvlco.com

All our training programs are also available in-house. To arrange an in-house program please **contact us on** :

+91-9764835350 or email info@mvlco.com

LIVE VIRTUAL CLASSROOM

Certification training is available in (a) live classroom mode (b) live virtual classroom mode (c) webinar mode (d) Studio recordings mode and (e) recorded classroom mode.

Certified Payment Messaging Expert (CPME)

MVLCO

Duration:
4 full days.

This course is conducted regularly at Bangalore, Mumbai, Hyderabad and Pune . We also conduct CPME in-house at client locations.

Why should you attend:
International and domestic payments are one of the most happening domain areas in banking and finance. Large opportunities exist for **Payment Professionals** in banks and IT/Software industry. After this certification you would have a cutting edge over others !

Course contents

Introduction to usage of messages in payment systems

- Overview of payments process including push/pull transactions
- Global formats e.g. SWIFT MT/ISO20022, ISO8583, EDIFACT
- Regional/proprietary formats e.g. UK Standard 18/60, USA ANSI
- Core data elements in payment messages

Overview of SWIFT MT messaging

- What is SWIFT
- Various products and services offered by SWIFT to banks/financial institutions and corporates
- SWIFT messaging services :
  - SWIFTNetFin, FileAct, InterAct and Browse
- Overview of SWIFT connectivity :
  - SNL, Alliance Gateway, Alliance Web Platform, Alliance Access, Alliance Lite and structures used in financial institutions
- Corporate connectivity :
  - SCORE, MA-CUG, TRCO
- Banking relationships e.g. Nostro/Vostro and corporate relationships
- SWIFT message routing restrictions and message user groups
- Understanding Relationship Management Application (RMA)
- Overview of SWIFT MT messages :
  - MT1XX to MT9XX, MTnXX,
  - System messages and Service messages, ACK/NAK, UAK. UNAK and notification messages
- Payment market practices and guidelines
- Institution identification : BIC Policy
- SWIFT MT message structure and message blocks

Using SWIFT FIN messages for payments

- Concepts, Terminology and understanding basic fields in SWIFT MT messages
- Understanding of important messages in MT1XX series:
  - Request for transfer : MT101
  - Multiple customer credit transfer : MT102
  - Single customer credit transfer : MT103 in serial mode and MT 103 with MT202COV in cover mode
  - Direct debit/request for debit : MT104
- Understanding of important messages in MT2XX series:
  - Financial institution transfer for own account : MT200
  - Financial institution transfer for own account : MT201
  - General financial institution transfer : MT202
  - Multiple general financial institution transfer : MT203
  - Financial markets direct debit : MT204
  - Financial institution transfer execution : MT205
  - Notice to receive : MT210
- Understanding of important messages in MT9XX series:
  - Confirmation of debit : MT900
  - Confirmation of credit : MT910
  - Request message : MT920
  - Customer statement message : MT940
  - Interim transaction report : MT942
  - Statement message : MT950

- **Use of SWIFT MT messages in End to end payment transaction processing : From remitter to beneficiary covering business scenarios of inward and outward payments.**

FSI ACADEMY

www.mvlco.com

Certified Payment Messaging Expert (CPME)

Course contents (Continued)

- SWIFT MT Reject, Return and transaction cancellation process
- Payment investigations : MT n92, n95, n96
- Message reconciliation and payment/nostro reconciliation process

SWIFT AML Sanctions

- How SWIFT sanctions is used in payment processing

MX Messaging (ISO20022 XML messages)

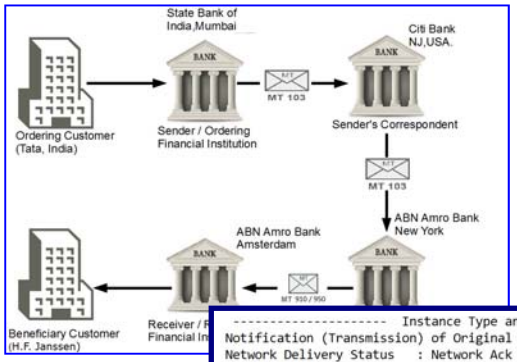
- Understanding the need for ISO20022 messages
- ISO20022 coexistence and convergence
- Overview of XML messages under ISO20022 used for payment transactions
- Structure of MX messages
- Overview of MX PACS, PAIN, CAMT messages for payments processing
- PACS (Payments Clearing and Settlement)
- PAIN series (Payment Initiation)
- CAMT series (Cash Management)
- Other relevant MX messages
- Use of ISO20022 MX messages in End to end payment transaction processing : From remitter to beneficiary covering business scenarios of inward and outward payments.
- Exceptions and investigations in payments using ISO20022 messaging

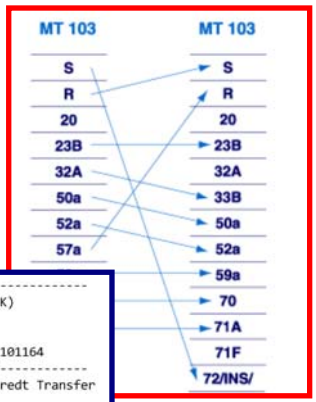
Overview of other standards for payment messaging

- United Nations EDIFACT messaging standard
- USA ANSI standard/X12/S820
  - USA Fedwire messages
  - USA CHIPS messages
- UK BACS Standard 18 file format and other reports

Basel III requirement of liquidity management

- Intraday liquidity management BCBS248






```
---------------------  Instance Type and Transmission --------------
Notification (Transmission) of Original sent to SWIFT (ACK)
Network Delivery Status   : Network Ack
Priority/Delivery         : Normal
Message Input Reference   : 1414 130626JIPBGBLNLAAXXX4462101164
---------------------------- Message Header -------------------------
Swift Input                  : FIN 103 Single Customer Credt Transfer
Sender   : JIPBGBLNLAXXX
           JAMES INDUSTRIAL BANK LIMITED
           LONDON UK
Receiver : CITIUS33XXX
           CITIBANK N.A.
           NEW YORK,NY US
--------------------------- Message Text ---------------------------
 20: Sender's Reference
     GTB170460A/13/FT
23B: Bank Operation Code
     CRED
32A: Val Dte/Curr/Interbnk Settld Amt
     Date           : 26 June 2016
     Currency       : USD (US DOLLAR)
     Amount         :                #5124,00#
50K: Ordering Customer-Name & Address
     /212760920210
     Morgon Automotive Corporation
```

FSI ACADEMY

www.mvlco.com

Certified Payment Messaging Expert (CPME)

MVLCO

Course modules

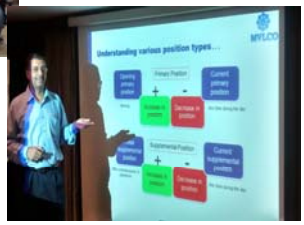
Module 1 : Introduction to payment messaging

Module 2 : Basics of SWIFT MT messaging

Module 3 : SWIFT MT messages for payments

Module 4 : ISO 20022 messages for payments

Module 5 : Other payment messaging standards



Get Certified ! Stay Ahead of the Competition !

FSI ACADEMY

www.mvlco.com

2018

MVLCO

Certified Card Payment Systems Professional (CCPSP)™

CCPSP certification will help you in enhancing your skills in Card Payment Systems. The certification will provide you with an insight in end-to-end card payment operations.

Get certified! Stay ahead of the competition!

MVLCO offers a four full days comprehensive CCPSP program extensively focused on Payment Card Systems. The course covers how payment cards e.g. credit/debit cards are issued, overview of EMV standards for Chip/ICC cards, how magstripe, Chip/NFC/RFID card transactions are processed , the use of Switch/HSM, Key Management, inter-bank settlements, merchant settlements and all important aspects of card payment processes.

The CCPSP program emphasizes on active participation from delegates and includes exercises and case studies.

When you complete CCPSP, you will have understanding of :

- Different types of payment cards
- Payment cards issuance process
- Role of various players in payment card industry
- Use of Switch, HSM and key management process
- End-to-end EMV/NFC/magstripe transaction processing
- ISO 8583, ASN.1/BER and ISO 20022 messages
- Frauds in card payment systems and card security
- Use of fraud management software in card industry
- International standards i.e. PCIDSS and EMV

Certification training is available in (a) live classroom mode (b) live virtual classroom mode (c) webinar mode (d) Studio recordings mode and (e) recorded classroom mode.

LIVE VIRTUAL CLASSROOM

Register today!

Must Do

A "Must Do" course for those wanting to work in Payment Card Industry

All our training programs are also available in-house. To arrange an in-house program please **contact us on** :

+91-9764835350 or email info@mvlco.com

Certified Card Payment Systems Professional (CCPSP)™

MVLCO

Duration:
4 full days.

This course is conducted in live classroom mode at Bangalore, Mumbai and Pune. The program is also available in live virtual classroom mode.

Why should you attend:
Card payments are very popular methods of making retail payments. CCPSP program will enable you to get thorough knowledge of how card payment systems operate, risks and opportunities in card payments and future of card payments.
Register today!!
Contact: +91-9764835350

Course contents

Introduction

- History of Payment Cards
- Players in Payment Card Industry
- Card payments life cycle
- Card Schemes
- Types of Cards
  - Products viz. credit card, debit card etc.
  - Physical ; Magstripe, ICC, Contactless, NFC, Virtual
  - Structure of cards : Magstripe, ICC, Contactless, NFC
  - PIN, CVV, iCVV, CVV2
- Access devices : ATM, POS terminal/M-POS, Internet and MOTO

Card Issue Process

- Card Types
- Track Types
- Chip card/RFID/NFC cards
- Secure Elements/Host Card Simulation
- EMV card/terminal specifications
- EVM ICC personalisation
- Card Production and PAN/CAF Generation for Switch
- PAN/CAF Upload in Switch
- PIN Generation and PIN Blocks

Electronic Fund Transfer Switch

- Introduction to Switch and its Functions
- Brief Introduction to Hardware Requirements
- Brief Introduction to Software Components

HSM and its Functions

- Host/Hardware Security Module
- Hardware Components
- Key Management Function
  - Local Master Keys
  - Zone Master Key
  - Zone PIN Key
  - Terminal Master Key
  - Terminal PIN Key
  - Terminal Authentication Key
  - PIN Verification Key
  - Card Verification Key
  - Master/Session Key Scheme
- Automated Key Distribution System

Introduction to Card Operations

- Introduction to ISO 8583, ASN.1/BER and ISO 20022 Messages.
- Functions of Issuer, Acquirer, Merchants and Inter-connect
- Revenue Streams
- Costs of Card Operations

Continued on next page

BFSI ACADEMY

www.mvlco.com

Certified Card Payment Systems Professional (CCPSP)™

MVLCO

Course contents (Continued)

Card Operations

- Overview of EMV standards
- EMV L1/L2/L3 Certification requirements
- Communication protocols T=0/T=1
- Kernels and Kernel Tags
- DE55 and ASN.1/BER Tags
- Permitted Transactions
  - Card Present Transaction (CP)
  - Card Not Present Transactions (CNP)
- Transaction flow for CP and CNP Transactions
  - Full EMV and Early/Quick EMV
  - Data Authentication : SDA/DDA/CDA
  - CVM/Offline/Online PIN verification
  - Accounting
  - Authorisations
  - Online/offline authorization processes e.g. PBF/SAF, Grading
  - EMV Commands and APDU Command/Response Pairs
  - EMV process of GENERATE 1st AC/GENERATE 2nd AC
  - Full STIP, Partial STIP, Co-operative Processing
- Reconciliations
  - Importance of Reconciliations
  - Various types of Reconciliations
- Customer Billing, Collection and Recovery
- Presentments and Chargebacks
- Settlements
  - VISA/Master Settlements
  - Partner Settlements
  - Merchant Settlements

Card Frauds and Security Issues:

- Card frauds
- Use of Applications for Fraud Detection and Prevention e.g. FICO Falcon

Card Standards

- Payment Card Industry Data Security Standards (PCI DSS)
- EMV Standards
- Other relevant ISO standards e.g. ISO9564

Card Analytics

- Card Analytics : TRIAD/Strategyware

Regulation

- Dodd-Frank, USA
- EPC regulation on mobile cards in European Union and SEPA Cards

MVL Consulting Private Limited
#17, Laxman Villa Condominium, Near Jog Hospital, Paud Road, Pune 411038 India
Telefax: +91-20-25466154, +91-20-25422874 Mobile: +91-9764835350

FSI ACADEMY

www.mvlco.com

All Payments Progams i.e. CIPSP, CPPS, CCPSP and CPME

MVLCO

Registration details and course fees

Duration and delivery mode: Each of our payment courses have individual duration of 4 full days.

These courses are delivered in live classroom mode at Bangalore, Mumbai, Pune and Hyderabad .

These program is also available in

- Classroom mode
- Live virtual classroom mode through GoToWebinar.
- Classroom recordings and
- Studio recordings

Course and examination fees for each program:

Delivery mode	Indian Citizens	Foreign Participants
Classroom	INR 25,000	USD 1,000
Live Virtual Classroom : GoToWebinar	INR 25,000	USD 1,000
Classroom recordings - 3 months validity	INR 20,000	USD 750
Studio recordings - 3 months validity	INR 20,000	USD 750

The above fees is excluding Goods and Services Tax (GST) @ 18%/ Applicable tax is payable additionally.

Certification fees include the tuition, full course material, on-line examination fees program and does not include accommodation, transport and any other costs. Terms and conditions apply for classroom recording and studio recordings. Full course fees is payable in advance in favor of "**MVL Consulting Private Ltd**." Remittance information is provided at the time of registration.

To register for the courses or to know more about our early bird discount and combo offers, please send an email to info@mvlco.com or call +91-9764835350.

Get Certified ! Stay Ahead of the Competition !

FSI ACADEMY

www.mvlco.com

CCPSP™

MVLCO

About MVL Consulting Private Limited

We are a BFSI consulting and training company. Founded in 1996, **MVLCO** has been operating as a professional consulting company since then. We bring to bear a wealth of practical professional expertise and experience of directly operating in banking and financial markets, and of providing relevant training. Our services include BFSI domain consulting services, business analysis services and information security (ISO27001).

We have gained expertise and experience in BFSI by our interactions and assignments with Central Banks, global commercial banks, merchant banks, fund management companies, stock exchange and its leading member firms and international consulting firms.

Our clientele includes Central Banks, global banks and multi-national IT companies.

CCPSP™

MVLCO

MVLCO is endorsed education provider of International Institute of Business Analysis (IIBA) and also a recognised training provider of International Requirements Engineering Board (IREB)

Our popular certification programs

Foundation Level Certifications

- Certified Banking Domain Professional (CBDP)
- Certified Requirement Engineering Professional (CPRE – International Board for Requirement Engineering)

Advanced Level Certifications / Courses

- Certified International Payment Systems Professional (CIPSP)
- Certified Payments Processing Specialist (CPPS)
- Certified Payment Messaging Expert (CPME)
- Certified Card Payment Systems Professional (CCPSP)
- Certified International Trade Finance Professional (CITFP)
- Certified Cards and Mobile Payments Professional (CCMPP)
- Business Analysis Professional (IIBA accredited course for CBAP/CCBA)
- Investment Banking and Integrated Treasury Operations
- Risk Management and Derivatives
- Many more……

Our certification programs are recognised for career development in many the global IT companies. Contact info@mvlco.com for more information on our certification programs.

IIBA Endorsed Education Provider™

IREB Recognized Training Provider 2017

Get certified, stay ahead of the competition

Certified Card Payment Systems Professional (CCPSP)™

MVL Consulting Private Limited

www.mvlco.com

2018

Program process

- Inter-active sessions
- Post program support
- Reviews/questions during the sessions
- If you do not understand, ask immediately
- Speed of delivery
- Mobile phones
- Session breaks
- Evaluation process

Program modules

- Module 1 : Basics of card payment systems
- Module 2 : Understanding card and PIN
- Module 3 : Before starting card operations
- Module 4 : ISO 8583 and ISO 20022 messages
- Module 5 : Transaction processing
- Module 6 : Card frauds, PCI DSS and EMV standards

Certified International Payment Systems Professional (CIPSP)™

Module 1
Basics of Card Payment Systems

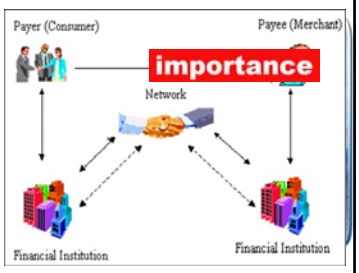
MVL Consulting Private Limited
www.mvlco.com

Module Objective

At the end of this module, you will understand:

1. *Brief history of card payment systems*
2. *Players in payment card industry and their roles*
3. *Card schemes and types of cards*
4. *Types of permitted transactions*

Key elements of payment



- **Message**
  - instructions or request to pay
- **Clearing**
  - message processing, may involve netting
- **Settlement**
  - exchange of value between parties

- A card payment transaction has all three elements
  - (1) Message (2) Clearing/Netting (3) Settlement
- **Payment system classification**
  - Whole sale and retail payment system
  - Real-time and batch payment system

H WHY? a

Brief history

- **1887** : The concept of using a card for purchases was described by Edward Bellamy in his utopian novel Looking Backward.
- **1921** : Western Union began issuing charge cards to its customers
- **1928** : The Charga-Plate, developed in 1928, was an early predecessor to the credit card and used in the U.S. from the 1930s to the late 1950s.
- **1950** : The concept of customers paying different merchants using the same card was expanded by Ralph Schneider and Frank McNamara, founders of Diners Club, to consolidate multiple cards.
- **1951** : The Franklin National Bank in New York formalized the practice and introduced credit cards.
- **1958** : Bank of America in Fresno, California launched blue, white and gold BankAmericard
- **1966** : The ancestor of MasterCard was born when a group of banks established Master Charge to compete with BankAmericard
- **1966** : Barclaycard in the United Kingdom launched the first credit card outside the United States.

Global associations

- In 1970, an association, National BankAmericard, Inc. (NBI), was formed of those U.S. banks issuing BankAmericards.
- In 1974, Bank of America's international licensees chartered an international company, IBANCO, to administer BankAmericard, Inc., outside the U.S.
- In 1976, IBANCO become Visa International and National BankAmericard, Inc. became Visa U.S.A.

- In 1966 16 banks come together in Buffalo, New York to form InterBank Card Association (ICA).
- In 1968, ICA went global by forming an association with Banco Nacional in Mexico and later, ICA formed alliance in Europe with Eurocard.
- By the late 1970s, ICA had members from as far as Africa, Asia and Australia.
- To reflect the commitment to international growth, in 1979 ICA changed its name to MasterCard International. In 2006, MasterCard International underwent another name change to MasterCard Worldwide.

Players in Payment Card Industry (PCI)

Cardholder/ Customer

Customer associated with the Primary Account Number (PAN) requesting the transaction from the card acceptor

Acquirer

A financial institution or it's agent which acquires from the card acceptor the data relating to transaction and initiates that data into an interchange system.

Interconnect/ Associations

Entities e.g. VISA, MasterCard, Rupay, Links, providing connectivity, clearing and settlement services among banks. Aggregators e.g. Paytm

Service Providers

Providing networking services, ATM maintenance services, cash vault and cash management services to financial institutions.

Manufactures and Developers

Card manufactures, device (ATM/POS) manufacturers, switch application developers, fraud application developers

Regulators

Payment system regulators e.g. Federal Reserve, Reserve Bank of India, PRA/FCA in UK. Card standards issuers e.g. PCIDSS, EMV, ISO8583/ISO20022

HONG KONG MONETARY AUTHORITY 香港金融管理局

BANK OF ENGLAND PRUDENTIAL REGULATION AUTHORITY

RESERVE BANK OF AUSTRALIA

Services provided by interconnects like VISA and MasterCard

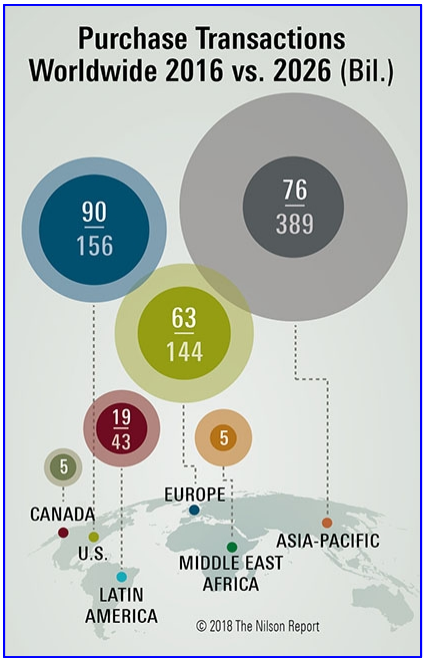
- A **clearing and settlement service** that processes transactions electronically between acquirers and card issuers to ensure that:
  - transaction information moves from acquirers to card issuers for posting to cardholders' accounts.
  - Payment for transactions moves from card issuers to acquirers to be credited to the merchants' accounts.

- An **authorization service** through which card issuers can approve or decline individual card transactions.
- Stand in processing (STIP) in certain cases.

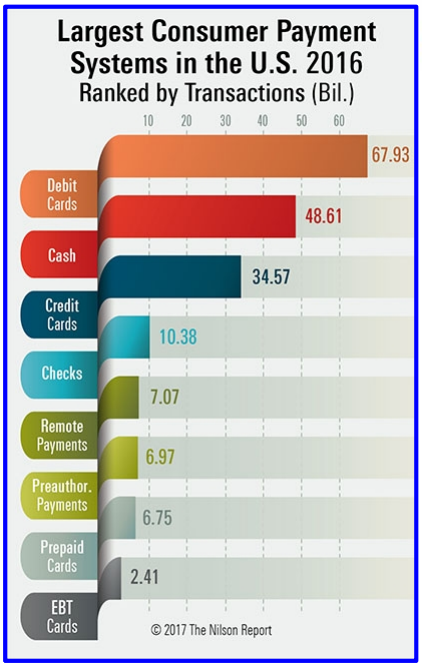
Clearing & Settlement

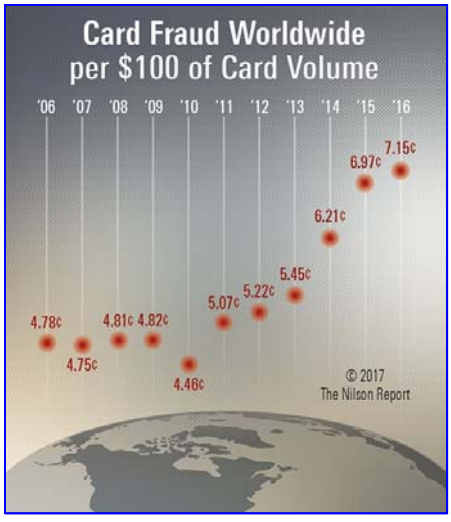
A brief overview of card industry

- **In 2026 global brand credit, debit, and prepaid cards are projected to reach 767 billion purchase transactions for goods and services worldwide.**
- **Global brand cards are Visa, Mastercard, UnionPay, American Express, Discover/Diners Club, and JCB.**



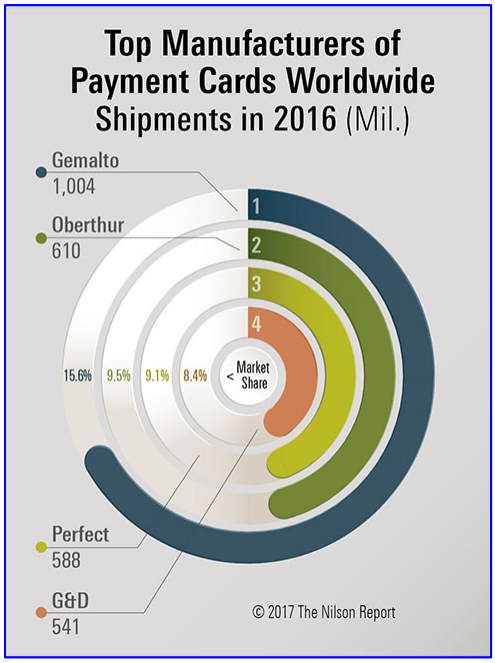
- U.S. Consumer Payment Systems are comprised of 11 instruments
- debit, credit, prepaid, and EBT cards,
- cash,
- checks,
- money orders,
- official checks,
- travel checks,
- preauthorized payments, and
- remote payments.

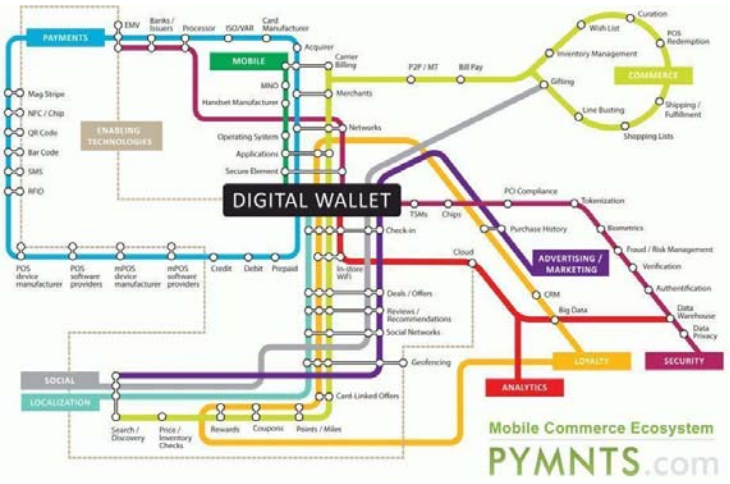




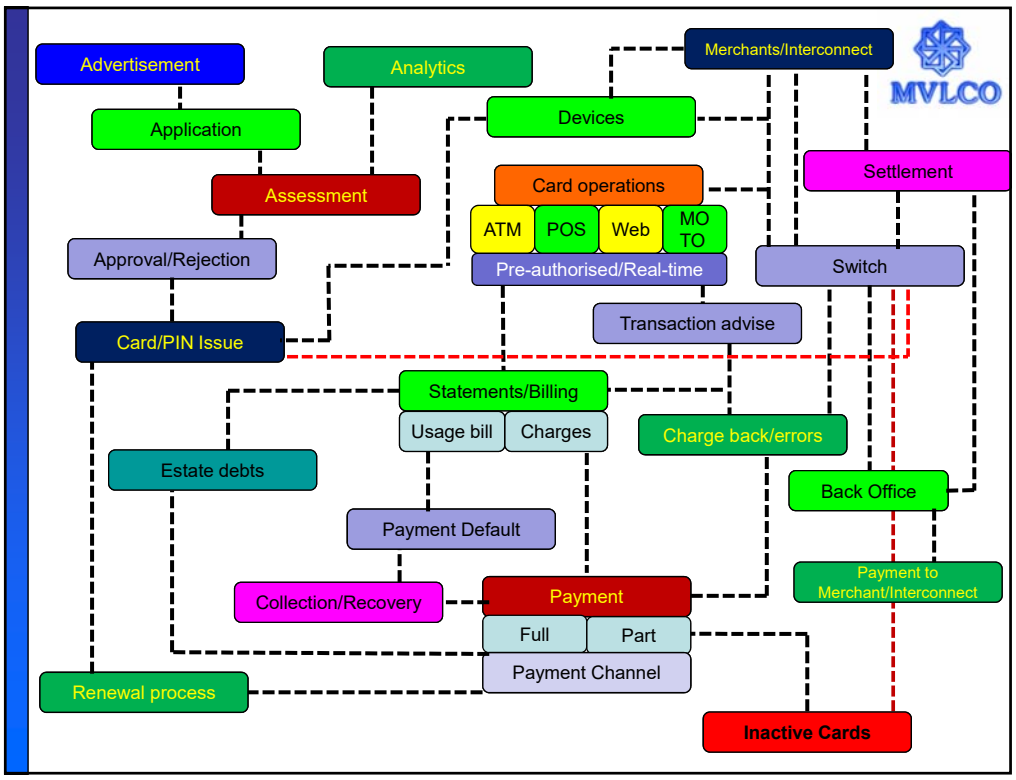
- Global card fraud in 2016 reached $22.80 billion. That figure amounted to 7.15¢ per every $100 in combined purchase and cash volume of $31.878 trillion.

- Manufacturers shipped more than 6.4 billion payment cards in 2016.
- The top suppliers were Gemalto, Oberthur, Perfect Plastic, and Giesecke & Devrient.





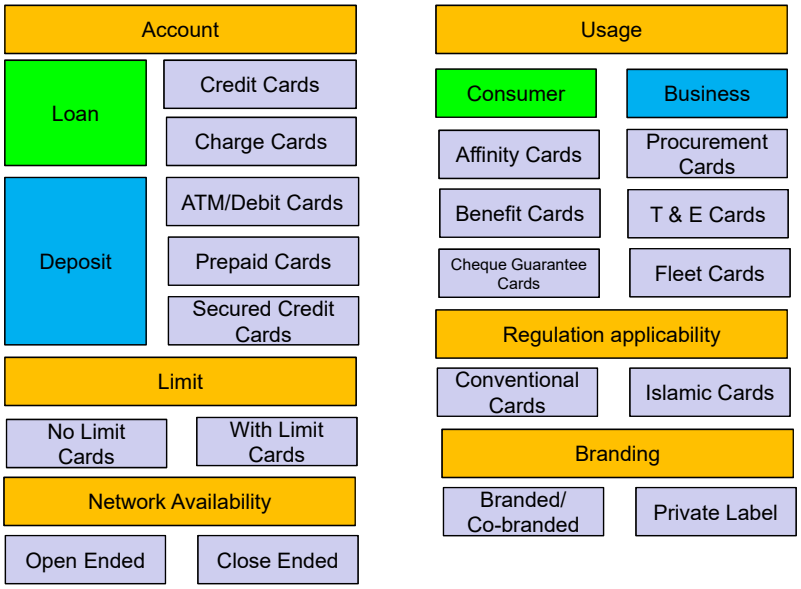
CREDIT CARDS (BROAD LEVEL) LIFECYCLE EVENTS



Card schemes

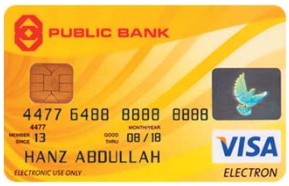
- **Three party scheme**
  - There is only one player dealing with the customer and the merchant
  - Example : American Express, Diners Club, Discover
- **Four party scheme**
  - Customer
  - Issuer
  - Acquirer
  - Merchant

Card classification



Various card brands

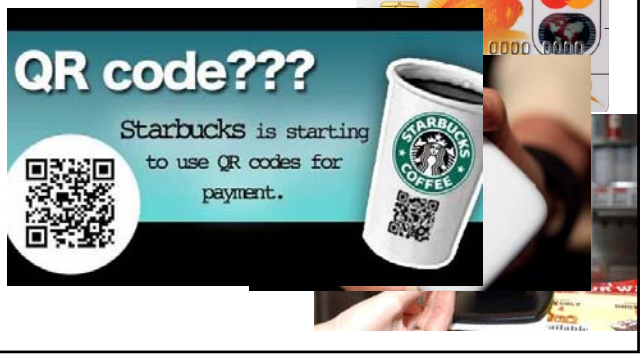
- Visa
- Visa Electron
- Visa Paywave
- MasterCard
- MasterCard Electronic
- MasterCard Maestro
- American Express
- Diners Club
- JCB
- Discover
- Rupay
- Many more….

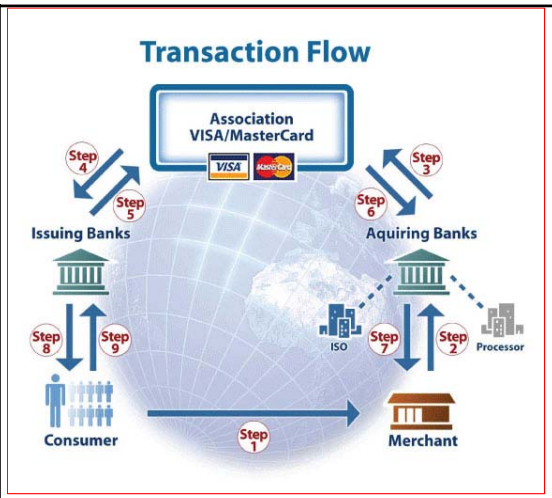


Card classification

ISO 7810/ISO 7816

- Magstripe Cards
- Smart Cards – Chip or ICC
- Contactless Cards
- NFC Cards
- Virtual Cards
- Quick Response Codes





MVLCO

PERMITTED TRANSACTIONS

MVLCO

Permitted transactions

- Cash Withdrawal from ATM
  - With card
  - Cardless
- Purchase of Merchandise
- Cash Out
- Internet Commerce
- Utility Payments
- Bill Payments
- Balance Transfers
- Fund Transfers
- Loan against Cards
- EMI transactions
- Cash advance cheque

Card Present (CP)

Card Not Present (CNP)

MVLCO

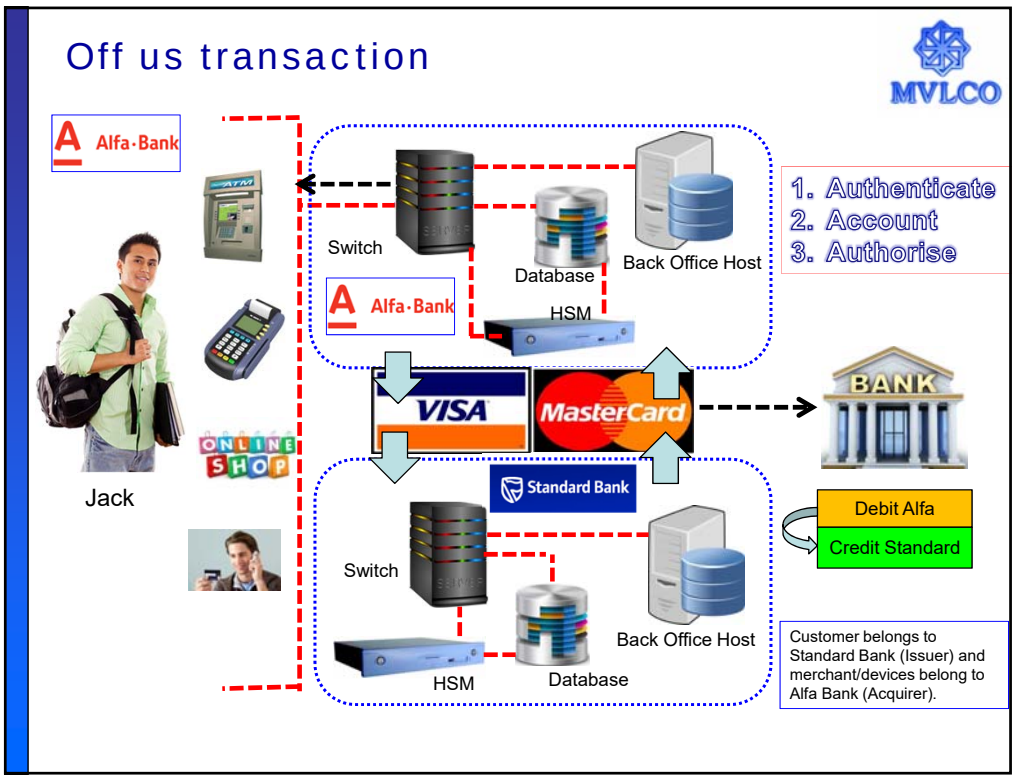
TRANSACTION PROCESS OVERVIEW

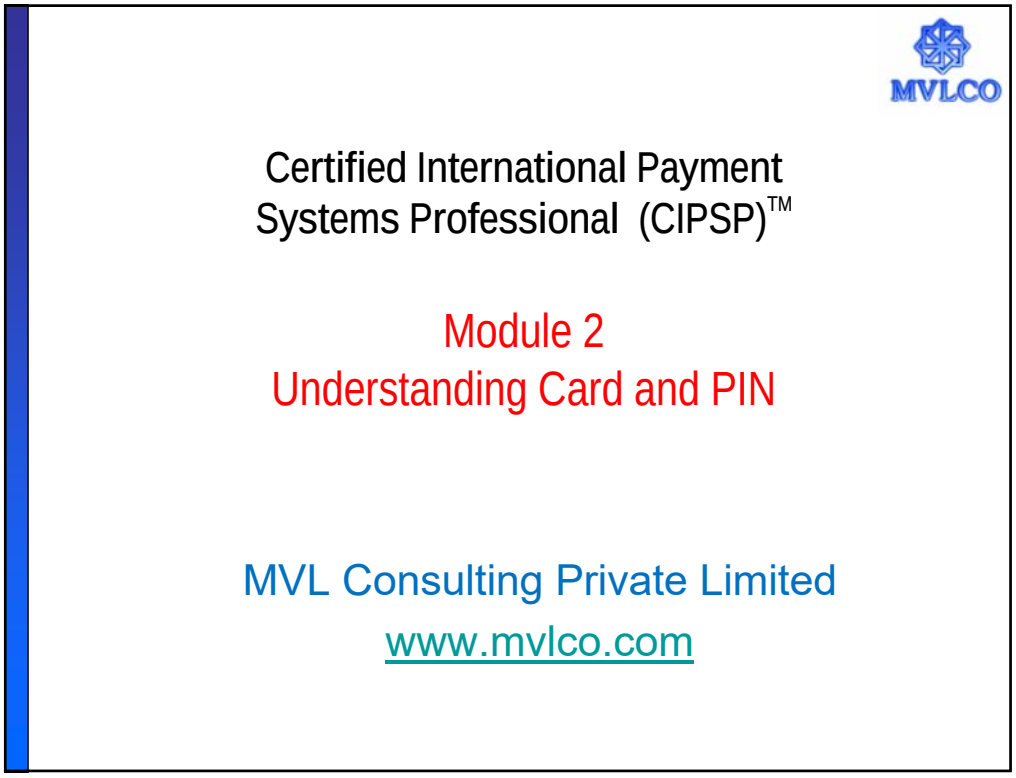
On us transaction

MVLCO

1. Authenticate
2. Account
3. Authorise

Customer and merchant/devices belong to the same bank.





Module Objective

At the end of this module, you will understand:

1. *Structure of cards*
2. *PIN generation and PIN Blocks*

INTERNATIONAL STANDARD

ISO/IEC 7810

Third edition
2003-11-01

AMENDMENT 1
2009-12-15

Credit cards are a common example of ISO/IEC 7810 ID-1 sized cards.

The standard defines four card sizes: ID-1, ID-2, ID-3 and ID-000.[3]

Format	Dimensions	Usage
ID-1	85.60 × 53.98 mm	Most banking cards and ID cards
ID-2	105 × 74 mm	French and other ID cards; Visas
ID-3	125 × 88 mm	Passports
ID-000	25 × 15 mm	SIM cards

All card sizes have a thickness of 0.76 mm (0.030 in).

ISSUER	IDENTIFIER	CARD NUMBER LENGTH
Diner's Club/ Carte Blanche	300xxx -- 305xxx, 36xxxx, 38xxxx	14
American Express	34xxxx, 37xxxx	15
VISA	4xxxxx	13,16
MasterCard	51xxxx -- 55xxxx	16
Discover	6011xx	16

MVLCO

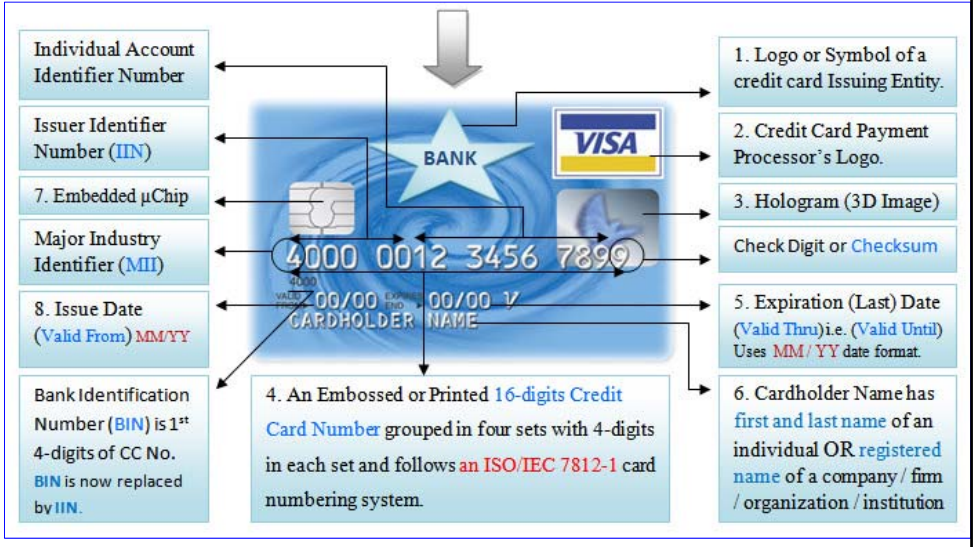
ISSUER IDENTIFICATION NUMBER

INTERNATIONAL STANDARD **ISO/IEC 7812-1**

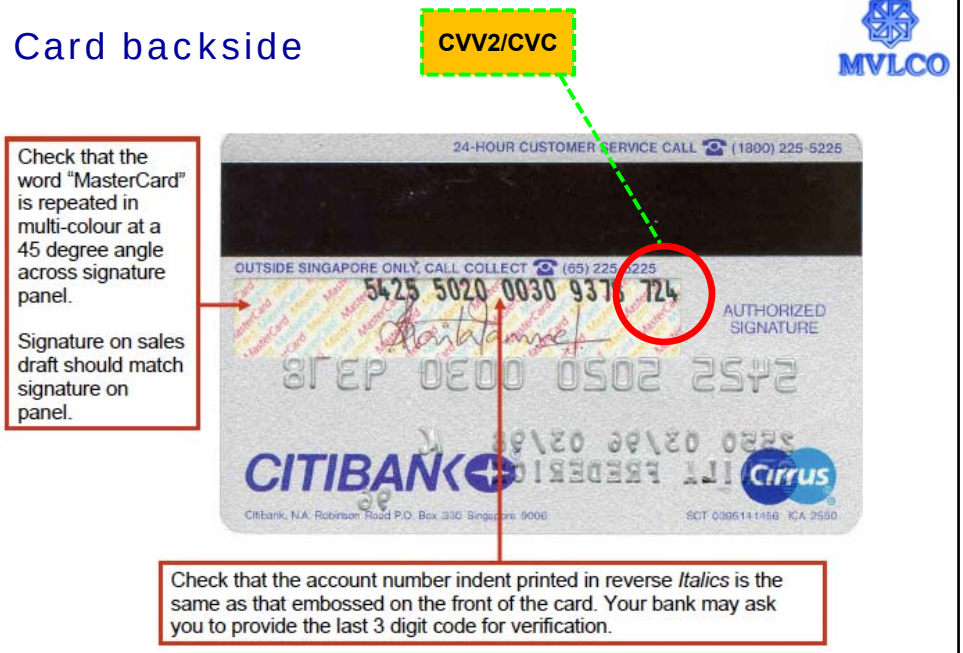
MVLCO

- The first 6 digits of a card number are known as the Issuer Identification Number (IIN), previously known as bank identification number (BIN).
- These identify the institution that issued the card to the card holder.
- Luhn Algorithm (mod 10) is used for number validation.

Card front



Card backside



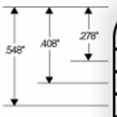
Card backside

Data Element	Track 1	Track 2
Start sentinel	X	X
Format code="B"	X	X
Primary account number	X	X
Field Separator	X	X
Name	X	
Field Separator	X	X
Expiration date	X	X
Service code	X	X
Discretionary data	X	X
End sentinel	X	X
Longitudinal redundancy check	X	X

CARD TRACKS DATA

Tracks on Plastic Card Magstrip

- There are three tracks on the magstripe. Each track is .110-inch wide. The ISO/IEC standard 7811, which is used by banks, specifies:
  - **Track one** is 210 bits per inch (bpi), and holds 79 six-bit plus parity bit read-only characters.
  - **Track two** is 75 bpi, and holds 40 four-bit plus parity bit characters.
  - **Track three** is 210 bpi, and holds 107 four-bit plus parity bit characters.
- Your card typically uses only tracks one and two. Track three is a read/write track (that includes an encrypted PIN, country code, currency units, amount authorized), but its usage is not standardized among banks.



0.223"			Recording Density (bits per inch)	Character Configuration (including parity bit)	Information Content (including control characters)
0.110"	Track 1	IATA	210 BPI	7 Bits per Character	79 Alphanumeric Characters
0.110"	Track 2	ABA	75 BPI	5 Bits per Character	40 Numeric Characters
0.110"	Track 3	THRIFT	210 BPI	5 Bits per Character	107 Numeric Characters

Figure A–1: Track 1 Record Format

Field Number	Length	Field Name
1	1	Start Sentinel
2	1	Format Code
3	13 or 16	Primary Account Number (PAN)
4	1	Separator
5	2 to 26	Cardholder Name
6	1	Separator
7	4	Card Expiration Date
8	3	Service Code
9	0 or 5	PIN Verification Position / Length / Content 1 / 1 / PIN Verification Key Index PVKI) 2 to 5 / 4 / PIN Verification Value (PVV)
10	Varies[1]	Discretionary Data
11	11[2]	Visa Reserved Position / Length / Content 1 to 2 / 2 / Zero fill 3 to 5 / 3 / Card Verification Value (CVV) 6 to 7 / 2 / Zero fill 8 / 1 / Authorization Control Indicator (ACI) 9 to 11 / 3 / Zero fill All 11 positions are required
12	1	End Sentinel
13	1	Longitudinal Redundancy Check (LRC)

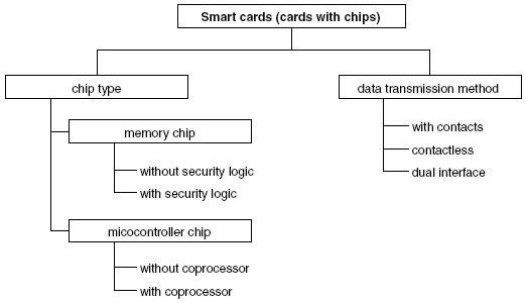
Table B–1: Track 2 Record Format

Field Number	Length	Field Name
1[1]	1	Start Sentinel
2	12–19	Primary Account Number (PAN)
3	1	Separator
4	4	Card Expiration Date
5	3	Service Code
6	0 or 5	PIN Verification Data
7	varies[2]	Discretionary Data[3]
8[1]		End Sentinel
9[1]	1	Longitudinal Redundancy Check (LRC)

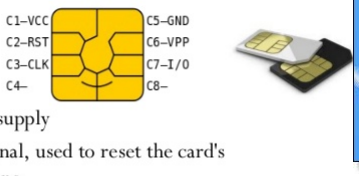
[1] Fields 1, 8 and 9 are not sent in online messages but are necessary for magnetic stripe-reading devices.
[2] The length depends on the lengths of fields 2 and 6. Refer to the Data Element Descriptions later in this appendix.
[3] Contains the 3-digit Card Verification Value (CVV) or optional iCVV on a chip.

Characteristics of ICC

- ICC is required to have physical characteristics as defined in ISO/IEC 7816-1. These are defined in EMV 4.3 Book 1.
- **Physical characteristics**
  - Module height
  - Dimensions and locations of contacts
  - Assignment of contacts
- **Electrical characteristics**
  - Temperature range
  - Input/output
  - Voltages



Micro module metallic chip design



- VCC: power supply
- RST: reset signal, used to reset the card's communications
- CLK: provides the card with a clock signal
- GND: ground (reference voltage)
- VPP: designated this as a programming voltage
- I/O: serial input and output (half-duplex).
- C4, c8: the two remaining contacts are used for usb interfaces and other uses

C1	Supply voltage (VCC)	C5	Ground (GND)
C2	Reset (RST)	C6	RFU [2]
C3	Clock (CLK)	C7	Input/output (I/O)
C4	Not used; need not be physically present	C8	Not used; need not be physically present

www.mvlco.com 43

Contactless and NFC cards

- Within EMV specifications, a card is considered to be any consumer token supporting contactless payment transactions, whether in the form of a payment chip card, a key fob, a mobile phone, or another form factor.
- From the perspective of a contactless reader, the other form factors communicate and behave the same as a contactless card that is compliant with EMV Book D.
- With respect to cardholder verification, mobile devices may take advantage of the user interface on the handset to allow cardholder verification of a contactless transaction by means of a confirmation code entered on the handset.
- **Some methodologies**
  - RFID
  - NFC
  - Near Sound Data Transfer (NSDT)
  - Bluetooth Low Energy (BLE)
  - Quick Response Codes

EMV®*
Contactless Specifications for Payment Systems

www.mvlco.com 44

CARD PERSONALISATION

Card personalisation

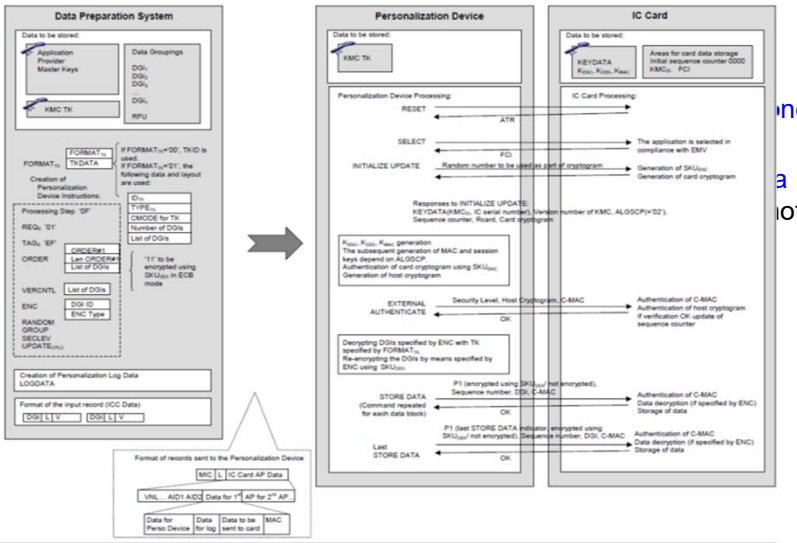
- Card personalization means the use of data personalization commands that are sent to a card that already contains the basic EMV application.
- This is sometimes referred to as “on-card” personalization.
- Within a personalization bureau environment the processing of Personalization Device Instructions (PDI) and IC card personalization data processing requires the following three functional steps:
  - Data preparation
  - Personalization device set-up and processing
  - IC card application processing.

M/Chip Advance Personalization Data Specifications

Card personalization methods

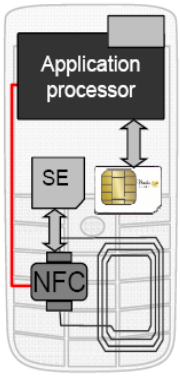
- **Indirect Method and Direct method**
- **The indirect method** assumes two security zones, one between the Data Preparation System and the Personalisation Device, and a second zone between the Personalisation Device and the ICC.
- **The direct method** assumes a single security zone between the Data Preparation System and the ICC. The Personalisation Device does not need to create APDU commands; it simply passes on the commands received from the Data Preparation System.

Card personalization methods

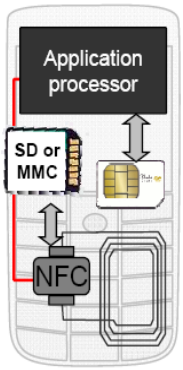


Secure NFC Architecture in Mobile Phones

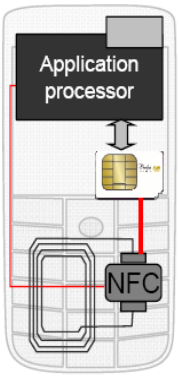
Secure element embedded in the phone



SD or MMC card hosting the application

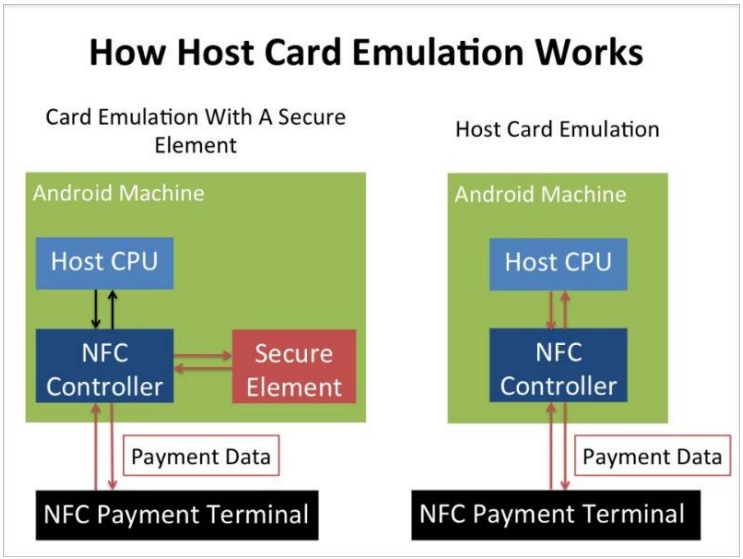


SIM centric solution



www.mvlco.com 49

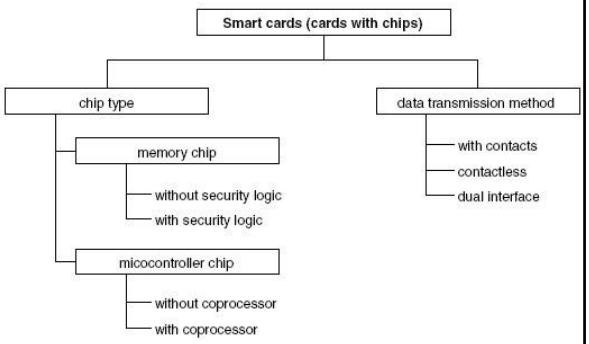
How Host Card Emulation Works



www.mvlco.com 50

Characteristics of ICC

- ICC is required to have physical characteristics as defined in ISO/IEC 7816-1. These are defined in EMV 4.3 Book 1.
- **Physical characteristics**
  - Module height
  - Dimensions and locations of contacts
  - Assignment of contacts
- **Electrical characteristics**
  - Temperature range
  - Input/output
  - Voltages



Card personalization validation

- The Card Personalization Validation (CPV) process generally consists of submitting a sample card for validation to a CPV Service Provider that tests it for conformance against the relevant personalization specifications.
- A sample card is a chip product representative of the Technical Product considered for issuance. As such it must be personalized with the same personalization profile and by the same personalization bureau that will be used for the personalization of the Technical Product in production mode. This process for submitting a sample card is detailed in Sample Submission.
- In some specific cases, the issuer may alternatively provide a list of minor changes that will be applied on a CPV-approved Technical Product, and request an assessment from a CPV Service Provider to be allowed deploying the modified Technical Product without having to submit a sample card. Accepted changes typically concern the addition of a new BIN, change of chip product to an equivalent chip product and minor changes on personalization parameter settings. If the result of the assessment is negative, the issuer is requested to perform a Sample Submission.

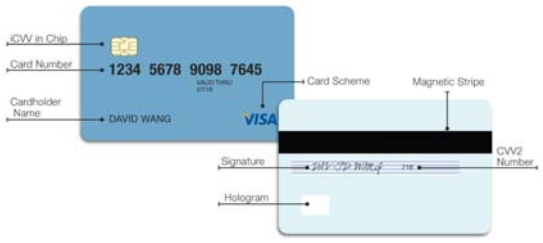
Process

www.mvlco.com 52

CARD VERIFICATION

CVV and iCVV

- The **CVV** is encoded on Track 1 and Track 2 in Magstripe or chip magstripe image.
- CVV provides a cryptographic check on the contents of magnetic stripe.
- The CVV is generated by using secret keys and algorithms chosen by the issuer. The algorithm is implemented in HSM or other facility designed for highly secret cryptographic operations.
- **iCVV** (integrated circuit card verification value) is an optional risk control feature that facilitates detection of skimmed chip data being used to counterfeit magnetic stripe cards.
- Contactless card and chip cards may electronically generate their own code viz. iCVV or Dynamic CVV, also known as Chip CVC (MasterCard) and



Generating CVV/iCVV

- The CVV computation uses DES/TDES issued by National Institute of Standards and Technology (NIST)
- One pair of 64 bit cryptographic keys called Card Verification Keys (CVKs) is used to generate and verify the CVVs.
- **The data elements needed to compute CVV/iCVV are**
  - Primary Account Number – 16 digit PAN
  - Card Expiration Date - YYMM format
  - Service Code – 3 digit
  - In iCVV computation, only the service code component in the data elements is changed to 999 instead of the actual service code.

CVV2

- CVV2 is a card verification tool designed to reduce fraud losses on CNP / MOTO transactions and also enhance the effectiveness of voice referrals.
- CVV2 is printed on back of the card.
- **The data elements needed to compute CVV2 are**
  - Primary Account Number – 16 digit PAN
  - Card Expiration Date
  - Service Code – 3 digit

INTERNATIONAL STANDARD **ISO 9564-1**

Banking — Personal Identification Number (PIN) management and security —

Part 1:
Basic principles and requirements for online PIN handling in ATM and POS systems

PERSONAL IDENTIFICATION NUMBER - PIN

PIN

- The minimum PIN length is 4 digits. For verification in interchange transactions, the maximum PIN length is 6 digits.
- An issuer can elect to support longer PINs upto a maximum of 12 digits as specified in **ISO 9564**.
- PIN types
  - Assigned derived PIN
  - Assigned random PIN
  - Customer selected PIN
- Implicit PIN activation/Explicit PIN activation
- A PIN used in interchange transactions must never be in a comprehensible (unencrypted) form except with a physically secure device such as HSM.

PIN block format examples

Format Value	Description
ECI-2	Eurocheque International format 2
ECI-3	Eurocheque International format 3
ISO-0	ISO format 0, ANSI X9.8, VISA 1, and ECI 1
ISO-1	ISO format 1 and ECI 4
ISO-2	ISO format 2
ISO-3	ISO format 3
VISA-2	VISA format 2
VISA-3	VISA format 3
VISA-4	VISA format 4
3621	IBM 3621 and 5906
3624	IBM 3624
4704-EPP	IBM 4704 with encrypting PIN pad

PIN block formats

- **ISO PIN Block Format 0**
  - This PIN Block format is based on the PIN, the PIN length, a subset of PAN and the pad characters of 0 and F, combined with an exclusive-or (XOR) operation.
- **ISO PIN Block Format 1**
  - This PIN block is constructed by concatenation of two fields: the plain text PIN field and the transaction field. It is used in situations where the PAN is not available.
- **ISO PIN Block Format 2**
  - The format 2 PIN block has been specified for local use with IC cards. The format 2 PIN block shall only be used in an offline environment and shall not be used for online PIN verification.
- **ISO PIN Block Format 3**

  This PIN Block format is identical for Format 0 except for the fill/pad digits.

ISO PIN Block Format 0 Example

The plain text PIN field shall be formatted as follows.

Bit

1	5	9	13	17	21	25	29	33	37	41	45	49	53	57	61	64
C	N	P	P	P	P	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	F	F	

where

C = Control field:	shall be binary 0000;
N = PIN length:	4-bit binary number with permissible values of 0100 (4) to 1100 (12);
P = PIN digit:	4-bit field with permissible values of 0000 (zero) to 1001 (9);
P/F = PIN/Fill digit:	designation of these fields is determined by the PIN length field;
F = Fill digit:	4-bit field value 1111 (15).

ISO PIN Block Format 0 Example

The account number field shall be formatted as follows.

Bit

1	5	9	13	17	21	25	29	33	37	41	45	49	53	57	61	64
0	0	0	0	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	

where

0 = Pad digit:	a 4-bit field with the only permissible value of 0000 (zero);
A1 ... A12 = Account number:	content is the 12 rightmost digits of the primary account number (PAN) excluding the check digit. A12 is the digit immediately preceding the PAN's check digit. If the PAN excluding the check digit is less than 12 digits, the digits are right justified and padded to the left with zeros. Permissible values are 0000 (zero) to 1001 (9).

PIN processes

- PIN Generation
- PIN Verification
- PIN Translation
- PIN Change
- PIN replacement

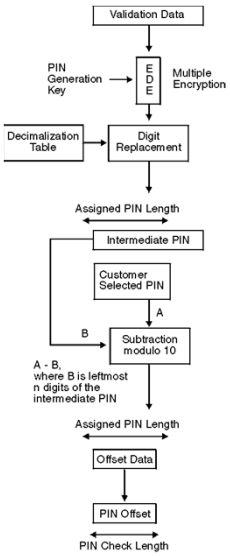
PIN Block Encryption

- All PINs in exchange messages must be encrypted before transmission.
- Certified PIN Entry Devices (PEDs) must be used.
- ATMs and POS PEDs must use approved reversible encryption algorithms to encrypt PINs.
  - Currently, the only approved algorithms are DES and TDES.

PIN Verification

- When a PIN is used, verification is performed by
  - **either** verifying the PIN data **online** against the issuer's database **or**
  - **offline** by using a Chip Card.
- When a **PIN** is to be **verified online**,
  - the PIN is entered, encrypted, transmitted, decrypted and compared to a reference PIN available only in the issuer's or agent's processing center.
  - If the PINs match, there is a high probability that the cardholder's identity has been verified.
- When a **PIN** is to be **verified offline**,
  - the PIN that is entered is compared to the Chip.
  - If the two PINs match, there is a high prob holder's identity has been verified.

IBM 3624 PIN and PIN Offset



- The IBM PIN calculation method produces a PIN that is 4 to 16 digits.
- The IBM PIN Offset calculation method is identical to IBM PIN calculation method except that there is an additional step after the PIN is generated to generate or use an Offset.
- To generate the Offset, the additional step subtracts, digit by digit, modulo-10, with no carry), the generated PIN from the customer selected PIN.

Certified International Payment Systems Professional (CIPSP)™

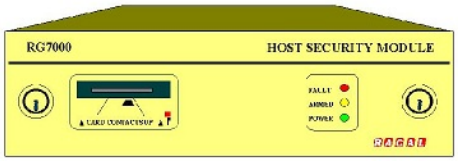
Module 3
Before Starting Card Operations

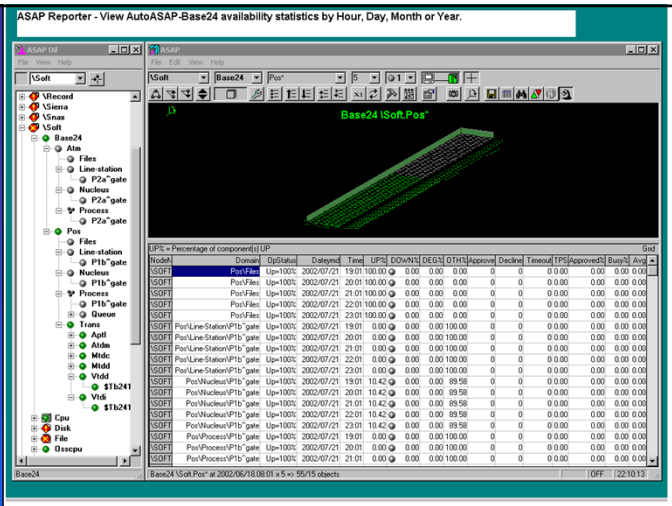
MVL Consulting Private Limited
www.mvlco.com

Module Objective

At the end of this module, you will understand:

1. *What is a switch and its functions*
2. *What is HSM and its functions*
3. *Key management*
4. *Different types of devices*
5. *Card issuance process*





MVLCO

BEFORE STARTING YOUR CARD OPERATIONS

Before starting card operations

MVLCO

- Switch
- Host – Core Banking Solution/Credit Card Server
- Host Security Module (HSM)/Software Security Module (SSM)
- Network
- Devices
  - ATM
  - POS
  - Websites
  - MOTO
- Card production and management system
- Authorisation management system
- Fraud management system
- FX rate feed system
- Billing system
- Call management system
- Cash management and forecasting software
- Backup system

PRODUCTION SET UP DOCUMENT FOR ABC BANK - VISA ISSUANCE

I. NEF Configuration:

1. **Station, Line and Process Creation.**
   a) IP address : 10.150.35.10
   b) Port : 8000
   c) Station Name: S1AABC BANKELEC
   d) Process Name: P1A^ABC BANKLEC
   e) Line Name: L1AABC BANKELEC

II. BASE24 Configuration:

1. **ICFE:**
   a. **FIID:** ABC BANK; **LNET:** ABC BANK
   b. **Issuer Station ID:** 8789906

ICFE Screen Settings:

```
SCREEN 1:

INTERCHANGE FIID: ABC BANK                    PROCESS: P1A^ABC BANKLEC

                    SWITCH TYPE: VISA
          INTERCHANGE LOGICAL NET: ABC BANK
                  REPORTING NAME: ABC BANK-REPORTS

                INSTITUTION ID: 40000000
                     SWITCH ID: 40000000
                     STATION 1: S1AABC BANKELEC
                     STATION 2:

                       SIC CODE: 0
                  CURRENCY CODE: 356  (IN)
              DEFAULT TERM NUM: S1AABC BANKELEC
        DEFAULT ACQUIRER ID NUM: 00935654545
       CUSTOMER BALANCE DISPLAY: 3  (DISPLAY AND PRINT)
```

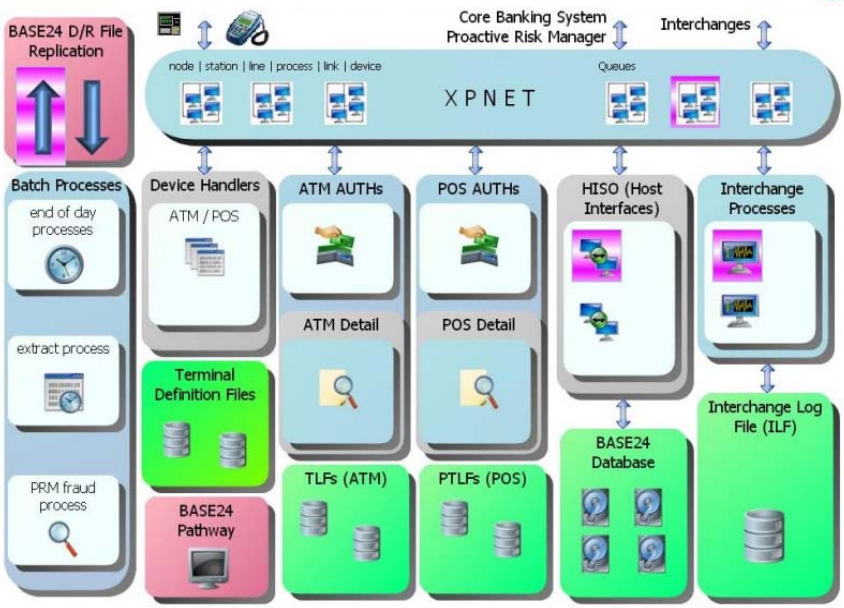
INTRODUCTION TO SWITCH

What is a SWITCH ?

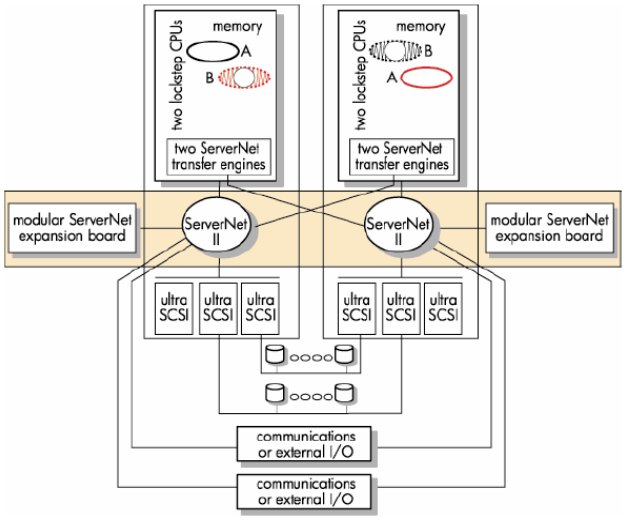
- **A switch is used for an integrated EFT processing and switching system that provides:**
  - device driving,
  - transaction routing and authorization,
  - host and interchange interfaces,
  - settlement, management reporting,
  - network control, and stored-value functionality.

Switch components

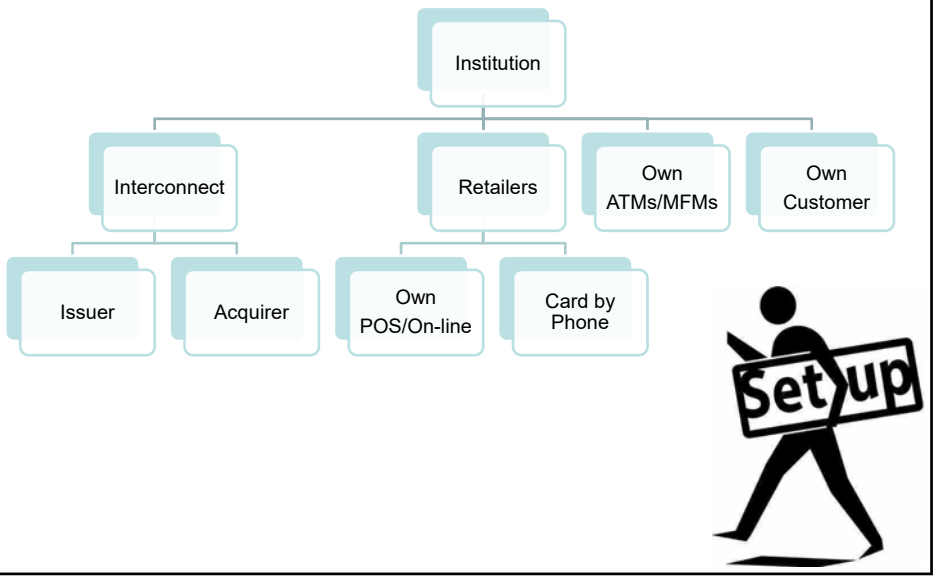
- **Channel Integrator -** Integration and management of various self-service channels e.g. ATM, POS, Internet Kiosk, Mobile.
- **Authorizing and Routing Engine –** Transaction authorization and routing between touch points and back end systems/external interchanges.
- **Host and Interchange Interfaces - Interface services** to all external systems, including customer back-end hosts, credit card systems, interchanges (VISA, MasterCard)
- **Monitoring Facility -** Systems monitor for the services and components, including maintaining information on the switching operations and performance.
- **Security Infrastructure -** Capability to transport transaction requests and response across channels and to authorization destinations in a completely secure manner.
- **Back Office -** Back office for card management, merchant management, interfaces to reconciliation and settlement with hosts, interchanges.
- **Device Handling/Management**



Basic two-processor NonStop system



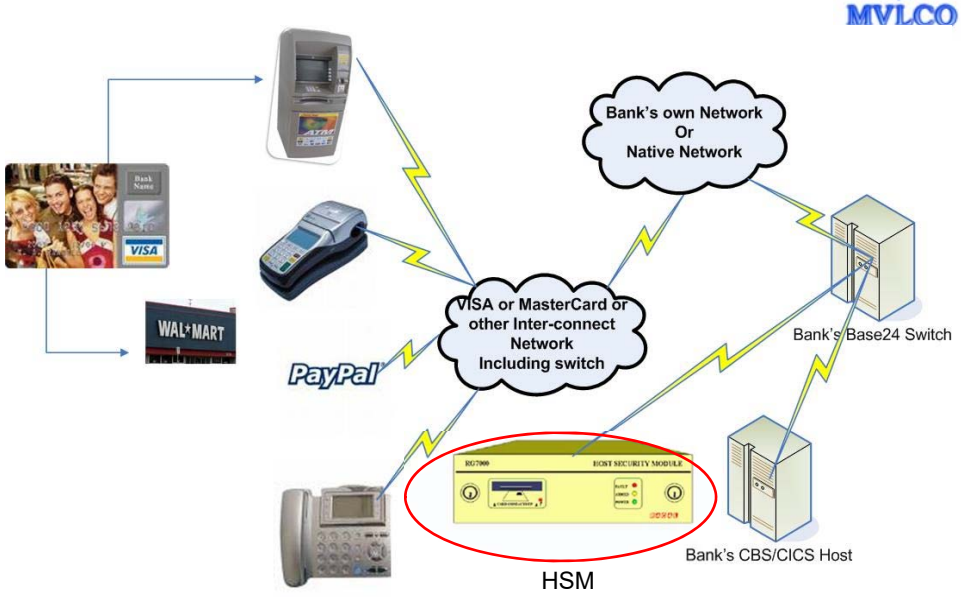
Initial set-up in a switch



MVLCO

HOST SECURITY MODULE

MVLCO



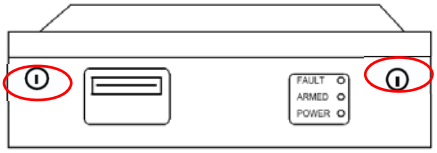
Host Security Module (HSM)

- **A Host Security Module - HSM** (also known as a Hardware Security Module) is an essential IT security element that provides cryptographic processing capabilities for a wide range of mission-critical applications used by banking, financial institutions, stock exchanges, governments, the military and many other industries.
- With increasing web-based threats and crimes, Host Security Modules are widely used to provide high-speed cryptographic processing services, secure key storage within a tamper-resistant platform.
- Some entities use Software Security Module (SSM) instead of HSM.

Host Security Module (HSM)

- **The HSM supports a number of standard functions and can be customised to perform client specific cryptographic functions.**
- **Standard functions include:**
  - Generating and verifying Personal Identification Numbers (PINs).
  - Generating encrypted card values such as Card Verification Values (CVVs)
  - Generating keys for use in Electronic Funds Transfer Point Of Sale (EFTPOS) systems.
  - Generating and verifying Message Authorisation Codes (MACs) for messages transferred via telecommunications networks.
  - Key management.

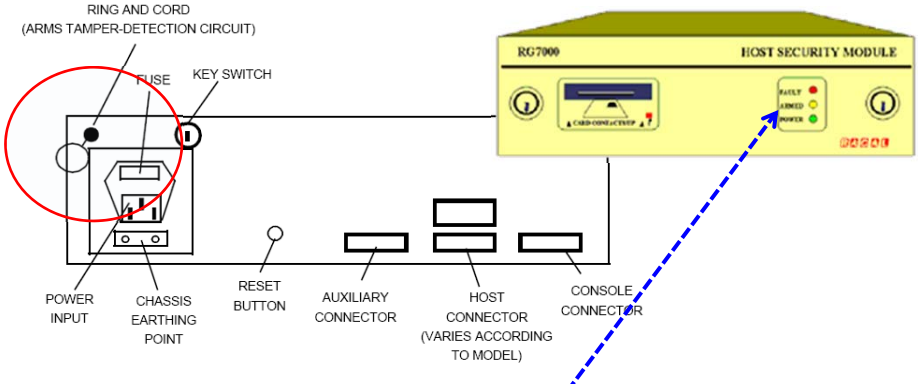
HSM Physical Security



THALES

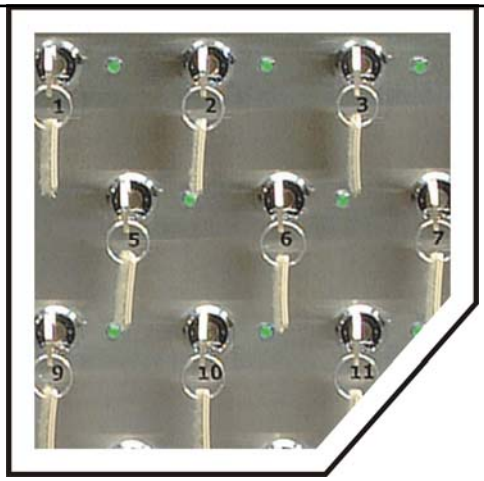
- The hinged front panel (see Figure) is secured by two cam locks.
- An HSM can be opened only when the two authorised key holders are present.
- After installation, it is not necessary to open the unit unless it requires maintenance (except to change the Local Master Keys (LMKs)).

HSM Physical Security



- The tamper-detection circuit is armed by a ring and cord: when the ring is pulled, it activates the detection circuitry, and pushing the ring cannot de-activate it. The ARMED indicator on the front panel illuminates when the ring has been pulled.

THALES



MVLCO

KEY MANAGEMENT

Key Management

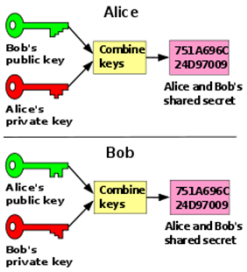
MVLCO

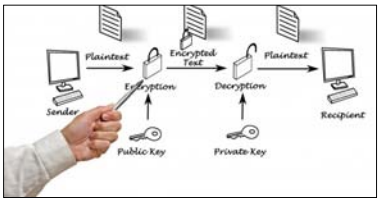
- The process of securely generating, distributing and storing DES/TDES keys and interconnect related keys is called the *Key Management*.
- **Master Keys**
  - Master keys are used to protect other keys for in-house storage.
  - This key is known only within a physically secure device at the member's processing center.
- **Key Exchange Keys (KEK)**
  - KEKs are used to encrypt and decrypt **working keys** so that they can be safely stored or conveyed from one network node to another network node.

Types of Keys

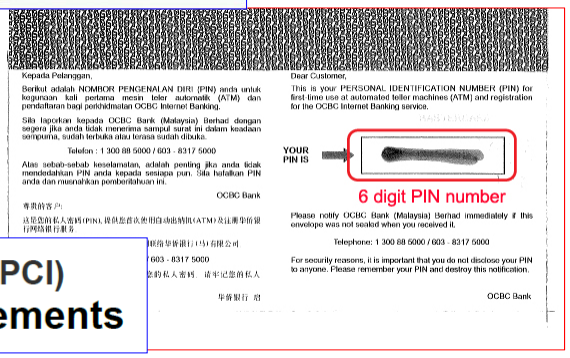
- Symmetric and asymmetric keys
- PKI : Public/Private Key Infrastructure
- Network Public/Private Key
- Issuer Public/Private Key
- EMV Card Public/Private Key

- Local Master Keys (LMKs)
- Zone Master Keys (ZMKs)
- Zone PIN Key (ZPK)
- Terminal Master Key (TMK)
- Terminal PIN Key (TPK)
- Terminal Authentication Key (TAK)
- PIN Verification Key (PVK)
- Card Verification Key (CVK)





PCI Security Standards Council™


Kepada Pelanggan,

Berikut adalah NOMBOR PENGENALAN DIRI (PIN) anda untuk kegunaan kali pertama mesin teller automatik (ATM) dan pendaftaran bagi perkhidmatan OCBC Internet Banking.

Sila laporkan kepada OCBC Bank (Malaysia) Berhad dengan segera jika anda tidak menerima sampul surat ini dalam keadaan sempurna, sudah terbuka atau terasa sudah dibuka.

Telefon : 1 300 88 5000 / 603 - 8317 5000

Atas sebab-sebab keselamatan, adalah penting jika anda tidak mendedahkan PIN anda kepada sesiapa pun. Sila hafalkan PIN anda dan musnahkan pemberitahuan ini.

OCBC Bank

Dear Customer,

This is your PERSONAL IDENTIFICATION NUMBER (PIN) for first-time use at automated teller machines (ATM) and registration for the OCBC Internet Banking service.

YOUR PIN IS

6 digit PIN number

Please notify OCBC Bank (Malaysia) Berhad immediately if this envelope was not sealed when you received it.

Telephone: 1 300 88 5000 / 603 - 8317 5000

For security reasons, it is important that you do not disclose your PIN to anyone. Please remember your PIN and destroy this notification.

OCBC Bank

Payment Card Industry (PCI)
PIN Security Requirements

Types of Keys used in HSM

Local Master Key

The Local Master Keys (LMKs) are a set of Data Encryption Standard (DES) keys stored in the HSM. All other keys and secret data are encrypted under the LMKs for local storage. Up to 20 pairs of LMKs are used with a triple encryption technique which effectively doubles the length of a standard DES key (making it 112 bits long).

For an HSM to operate, the LMKs must be created and loaded. Because the DES algorithm depends on a key for secrecy, and because the security of all keys and data encrypted for storage depend on the LMKs, they must be created and maintained in a secure manner. Provision is made to allow the LMKs to be changed and keys or data encrypted under them to be translated to encryption under the new LMKs.

All keys when stored locally (i.e. not in transit between systems) are encrypted under the LMK.

Zone Master Key

A Zone Master Key (ZMK) is a key-encrypting key which is distributed manually between two (or more) communicating sites, within a shared network, in order that further keys can be exchanged automatically (without the need for manual intervention). The ZMK is used to encrypt keys of a lower level for transmission. For local storage, a ZMK is encrypted under one of the LMK pairs.

Within the VISA environment this is known as a ZCMK.

Zone PIN Key

A Zone PIN Key (ZPK) is a data encrypting key which is distributed automatically and is used to encrypt PINs for transfer between communicating parties (for example, between acquirers and issuers). For transmission, a ZPK is encrypted under a ZMK; for local storage it is encrypted under one of the LMK pairs.

Terminal Master Key

A Terminal Master Key (TMK) is a key-encrypting key which is distributed manually, or automatically under a previously installed TMK. It is used to distribute data-encrypting keys, within a local (non-shared) network, to an ATM or POS terminal or similar. The TMK is used to encrypt other TMKs or keys of a lower level for transmission. For local storage, a TMK is encrypted under one of the LMK pairs.

Terminal PIN Key

A Terminal PIN Key (TPK) is a data-encrypting key which is used to encrypt PINs for transmission, within a local network, between a terminal and the terminal data acquirer. For transmission, a TPK is encrypted under a TMK; for local storage it is encrypted under one of the LMK pairs.

Types of Keys used in HSM

Terminal Authentication Key

A Terminal Authentication Key (TAK) is a data-encrypting key which is used to generate and verify a Message Authentication Code (MAC) when data is transmitted, within a local network, between a terminal and the terminal data acquirer. For transmission, a TAK is encrypted under a TMK or ZMK; for local storage it is encrypted under one of the LMK pairs.

PIN Verification Key

A PIN Verification Key (PVK) is a data-encrypting key which is used to generate and verify PIN verification data and thus verify the authenticity of a PIN. For transmission, a PVK is encrypted under a TMK or under a ZMK; for local storage, it is encrypted under one of the LMK pairs.

Card Verification Key

A Card Verification Key (CVK) is similar to a PIN Verification Key, but for Card information instead of a PIN

MVLCO

DEVICES INCLUDING ATM AND TERMINALS

MVLCO

Choose "Cash" and insert all your bills at once (up to 99 bills).