Securing Mobile Payment Protocol
based on EMV Standard

Mohammad Sifatullah Bhuiyan

Master of Science Thesis
Stockholm, Sweden 2012
TRITA-ICT-EX-2012-308
Acknowledgement

Foremost, I would like to express my thanks and deep gratitude to my supervisor Prof. Sead Muftic for his patience, motivation, guidance and sharing his immense knowledge to perform this research work.

Beside my supervisor, I would also like to thank the whole SecLab Team for their help and encouragements, which made my research time really enjoyable.

Finally thanks to my parents for their motivation, encouragement and support without which it would have been impossible to reach this stage.
Dedication

To my Parents,

Md. Safiullah Bhuiyan
&
Mrs. Nargis Akhter
Abstract

This is an era of communication technology. This era has faced a lot of innovation in technology sector. Mobile phones were once used for calling or text messaging only, now slowly becoming competitor of computers. The rapid development of hardware, software and operating system of smartphones made it possible to do multiple tasks through the phones.

Nowadays, smart phones have powerful operating systems which provide wide range of applications. Smart phones can be interfaced with external hardware also. The payment industry is about to see a drastic change because of these features. People can now pay through their smartphones; they can use payment cards to pay through it etc. But financial transaction is a very sensitive service and security is very crucial here. For financial services, the major security services such as confidentiality, integrity, authenticity, authorization and non-repudiation must be ensured.

There are two major types of payment cards, magnetic-stripe based cards and chip based cards. Chip based card provides better security. Magnetic stripe based cards being static, is easy to counterfeit. But the fact that these magnetic stripe cards are still used in many countries, it is necessary to provide a security solution in order to protect customers from treachery.

In this thesis, it has been investigated how to secure the mobile payment based on EMV standard. EMV is a chip based payment card. It has strong security features which made skimming or tampering it very hard. But, Magstripe based payments still remained insecure. This thesis paper aims to secure the transaction when paid with magnetic stripe based cards. Several measures have been taken to ensure that major security services are met. In addition, a prototype was developed and tested to demonstrate the practicality of the designed solution.

The research results of this paper show that by transacting through the secured mobile payment protocol, customers can avail payment service more securely than traditional magnetic striped card based payments.

Keywords: Mobile Payment Security, EMV, Magnetic Stripe.
Table of Contents

Acknowledgement ........................................................................................................... 2
Dedication ......................................................................................................................... 3
Abstract ............................................................................................................................. 4
Table of Contents ............................................................................................................... 5
List of Figures .................................................................................................................... 7
List of Tables ..................................................................................................................... 8
Abbreviations .................................................................................................................... 9

Chapter 1: Introduction ...................................................................................................... 11
  1.1 Background .................................................................................................................. 11
  1.2 Motivation and Goal .................................................................................................... 12
  1.3 Problem Statement ..................................................................................................... 12
  1.4 Methodology ............................................................................................................... 13
  1.5 Scope and Limitations ............................................................................................... 14
  1.6 Structure of The Report ............................................................................................ 14

Chapter 2: Transactions and Security .............................................................................. 15
  2.1 Magnetic Stripe Cards .............................................................................................. 15
    2.1.1 Transaction flow of credit & debit card. ............................................................... 18
    2.1.2 Security Vulnerabilities of Magnetic Stripe ....................................................... 18
  2.2 EMV Transaction ...................................................................................................... 19
  2.3 Security Basics .......................................................................................................... 22
    2.3.1 Attacking through forcing to Fall-back ............................................................... 24

Chapter 3: EMV Standard ................................................................................................ 25
  3.1 Why Magnetic Stripe-based Solution? ..................................................................... 25
  3.2 EMV Security ............................................................................................................ 26
    3.2.1 Card Authentication Method ............................................................................. 26
      3.2.1.1 Online Card Authentication ........................................................................ 26
      3.2.1.2 Offline Card Authentication ....................................................................... 26
    3.2.2 Card Holder Verification Method ........................................................................ 28
    3.2.3 Key Management ................................................................................................. 30
    3.2.4 EMV Offline Transactions Risk Management .................................................... 36

Chapter 4: Overview of Security Services in Mobile Environments .................................. 38
  4.1 PKI Overview ............................................................................................................ 38
    4.1.1 Mobile PKI .......................................................................................................... 39
    4.1.2 WAP based PKI ................................................................................................... 40
  4.2 SAFE System Overview ............................................................................................. 41
Chapter 5: Securing Magnetic Stripe Card-Data based on EMV Standard ...... 43

5.1 Online Card-Data Authentication of Magnetic Stripe ......................................... 44
5.2 Offline Card-Data Authentication of Magnetic Stripe ........................................ 45
  5.2.1 Authenticating Card-Data by Offline SDA .................................................. 46
  5.2.2 Authenticating Card-Data by Offline DDA .................................................. 47
5.3 Cardholder Verification ...................................................................................... 48
5.4 Key Management ............................................................................................... 50
5.5 Risk Management .............................................................................................. 50
5.6 Analysis and Conclusions ................................................................................ 50
5.7 Prototype ............................................................................................................ 51
  5.7.1 Implementation ............................................................................................ 52
  5.7.2 Summary ...................................................................................................... 54
  5.7.3 Analysis and Conclusions ........................................................................... 54

Chapter 6: Conclusions and Future Works ............................................................ 55

6.1 Conclusions ....................................................................................................... 55
6.2 Future Works ..................................................................................................... 56

References .............................................................................................................. 57
## List of Figures

<table>
<thead>
<tr>
<th>Figure No</th>
<th>Title</th>
<th>Page No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 1</td>
<td>Reasoning in the Design Cycle</td>
<td>13</td>
</tr>
<tr>
<td>Figure 2</td>
<td>Reverse Flux Creation at Trailing Border</td>
<td>15</td>
</tr>
<tr>
<td>Figure 3</td>
<td>Data Frequency and Pattern.</td>
<td>16</td>
</tr>
<tr>
<td>Figure 4</td>
<td>ANSI/ISO BCD Data Format</td>
<td>16</td>
</tr>
<tr>
<td>Figure 5</td>
<td>Credit Card Transaction</td>
<td>18</td>
</tr>
<tr>
<td>Figure 6</td>
<td>An Example of EMV Transaction Flow</td>
<td>19</td>
</tr>
<tr>
<td>Figure 7</td>
<td>AID and Corresponding Card Schemes</td>
<td>20</td>
</tr>
<tr>
<td>Figure 8</td>
<td>Offline Static Data Authentication</td>
<td>27</td>
</tr>
<tr>
<td>Figure 9</td>
<td>Offline Dynamic Data Authentication</td>
<td>28</td>
</tr>
<tr>
<td>Figure 10</td>
<td>Mobile PKI Authentication Steps</td>
<td>40</td>
</tr>
<tr>
<td>Figure 11</td>
<td>Authentication through WPKI</td>
<td>40</td>
</tr>
<tr>
<td>Figure 12</td>
<td>Ensuring Authentication and Integrity of Merchant and Card.</td>
<td>44</td>
</tr>
<tr>
<td>Figure 13</td>
<td>Design of Static Data Authentication for Magstripe Card-Data.</td>
<td>46</td>
</tr>
<tr>
<td>Figure 14</td>
<td>Design of Dynamic Data Authentication for Magstripe Card-Data.</td>
<td>47</td>
</tr>
<tr>
<td>Figure 15</td>
<td>Card Holder Verification with Enciphered PIN</td>
<td>49</td>
</tr>
<tr>
<td>Figure 16</td>
<td>Transaction from Customer’s Account to Merchant’s Account Taking Place in the Prototype.</td>
<td>53</td>
</tr>
</tbody>
</table>
# List of Tables

<table>
<thead>
<tr>
<th>Table No</th>
<th>Title</th>
<th>Page No:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table 1:</td>
<td>Format and Description of Track 1.</td>
<td>17</td>
</tr>
<tr>
<td>Table 2:</td>
<td>Format and Description of Track 2.</td>
<td>17</td>
</tr>
<tr>
<td>Table 3:</td>
<td>CVM Codes and Methods</td>
<td>29</td>
</tr>
<tr>
<td>Table 4:</td>
<td>Data Elements in the ICC for SDA Method</td>
<td>30</td>
</tr>
<tr>
<td>Table 5:</td>
<td>Required ICC Data Elements for Offline Dynamic Data Authentication</td>
<td>31</td>
</tr>
<tr>
<td>Table 6:</td>
<td>Data Objects Required for Offline DDA</td>
<td>33</td>
</tr>
<tr>
<td>Table 7:</td>
<td>Recovered Data Format from Issuer PKC</td>
<td>35</td>
</tr>
<tr>
<td>Table 8:</td>
<td>Dynamic Application Data to be Signed.</td>
<td>36</td>
</tr>
<tr>
<td>Table 9:</td>
<td>Comparing Mobile POS and Traditional POS</td>
<td>43</td>
</tr>
<tr>
<td>Table 10:</td>
<td>Description of Resources Used.</td>
<td>51</td>
</tr>
</tbody>
</table>
Abbreviations

ARPC  Authorisation Response Cryptoagram
ARQC  Authorisation Request Cryptoagram
ATM   Automated Teller Machine
CA    Certificate Authority
CAD   Card Accepting Device
C-APDU Command APDU
CDA   Combined DDA/Application Cryptoagram Generation
DDA   Dynamic Data Authentication
DDOL  Dynamic Data Authentication Data Object List
DES   Data Encryption Standard
GSM   Global System for Mobile Communications
ICC   Integrated Circuit Chip
NFC   Near Field Communication
OS    Operating System
OTP   One-Time Password
PIN   Personal Identification Number
PKI   Public Key Infrastructure
SAFE  Secure Applications for Financial Environments
SDK   Software Development Kit
SIM   Subscriber Identity Module
SP    Service Provider
RID   Registered Application Provider Identifier
RSA   Rivest, Shamir, Adleman Algorithm
SCA   Certification Authority Private Key
SDA   Static Data Authentication
SHA-1 Secure Hash Algorithm 1
SI    Issuer Private Key
SIC   ICC Private Key
PAN   Primary Account Number
PCA   Certification Authority Public Key
PI    Issuer Public Key
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIC</td>
<td>ICC Public Key</td>
</tr>
<tr>
<td>PIN</td>
<td>Personal Identification Number</td>
</tr>
<tr>
<td>POS</td>
<td>Point of Service</td>
</tr>
</tbody>
</table>
Chapter 1: Introduction

1.1 Background

Transaction started in human life in the form of exchange of goods according to necessity. People started using physical money after that. With the advancement of time and evolution of technologies, now money took electronic form. Popularity gradually increased to pay with the payment cards until m-Payment acceded in the industry.

M-payment also went under an evolution. Initially mobile phones with limited capabilities used the SMS services with the help of operator to complete the payment cycle. It became successful in some parts of World and is still popular in few countries. But SMS based mPayment system has very limited freedom of payment. This is a service provided by the Operator. Money is deducted from the balance of customer. Electronic money is not directly involved here. So customer can only do this payment where the merchant is in some form of agreement with the Operator, thus the freedom of payment in context of place and service is absent. SMS based payment is based on sending a specific SMS code, which not only limits the diverse payment options, but also lacks user friendliness. Besides, message delivery is not guaranteed every time. With the rise of smart phone and development of payment applications for smart phone, the popularity of mPayment got a new momentum. New technologies such as magnetic stripe, Bluetooth, NFC etc. are being utilized to integrate and facilitate smart phone payment. Same payment cards that people used in point-of-sales (PoS) devices are now being used through smart phones. The integration of regular payment cards and smart phone gave the world a new dimension of seamless payment. Magnetic stripe card reader for smart phone is a device which is used to read data of payment cards which is later processed in the smart phone. Usually it is an external device.

A rapid approach of electronic payment is lowering the maintenance cost and saving a great deal of time. But still there are obstacles due to lack of user friendliness in the technology. This approach is hindering the growth of Business-to-Customer relation of e-Commerce, and now a days, m-Commerce. Another reason being security flaws, users are afraid to use the technologies that are prompt to security vulnerability. There are lot of standards and protocols for the m-commerce for logistics, security etc. Having no reliable and standard was one of the biggest obstacles in the growth of mobile payment industry [4].

Upon the arrival of IPhone in the market, there has been a rapid expansion in smart phone market from other manufacturers also. The hardware as well as the operating systems was also developed to utilize the processing capabilities. One of the emerging and most promising operating systems for smart phone is Android. This OS is used not only in smartphones, but also in tablet and few other portable devices. Many organizations such as Banks made their website mobile phone friendly, so eventually mobile or smart phones are bringing the web even closer [3].

Another drastic change which is taking place is the payment area. Transactions through hard cash are well known method from very primitive time. Now alternative form of payment which is electronic payment is getting popular throughout the World. Payment through the
smartphone is a new concept which is very promising. This approach increases the mobility and interaction. The only problem that can hinder the popularity is security vulnerability. Traditional method of electronic money transfer was through magnetic card swapping. But due to its security limitations, more strongly secured and dynamic card appeared in the payment industry called EMV.

EMV (Europay, MasterCard and Visa) is an international standard for transactions between payment cards and point of sales. Payment can be done by contact oriented (e.g. by magnetic stripe) or contactless methods (e.g. by EMV stored in the mobile wallet via NFC technology). EMV technology is considered secure than traditional magnetic stripe, but this thesis discusses how to make magnetic stripe more secure using the security scheme EMV is using. As there are huge numbers of POS devices in the market which still accept magnetic swiping technologies, it is obvious to introduce strong security till magnetic stripe swipe technology finds itself into the history book. A secured solution, based on globally accepted EMV standard, assures the mass acceptance of considering this magnetic stripe based mobile payment protocol as a standard.

1.2 Motivation and Goal

Information is considered as one of the most valuable assets in today’s World. With incrimination of communication technology, the medium of data transmission is also increasing. If careful measures are not taken, valuable information can be intercepted. A technology which is vulnerable to security will not be popular in the competitive market. To maintain the popularity of mobile payment, it is thus necessary to provide a complete secured solution. The swiping technology of magnetic stripe is still popular because it is easy and relatively cheap to implement. But there are security threats in comparison to other similar payment technologies such as Chip and PIN based mPayment.

The goal of this thesis is to design a security protocol for magnetic stripe based mPayment, which protects customer and his data by considering the security issues: confidentiality, integrity, authenticity, authorization and non-repudiation.

1.3 Problem Statement

According to APACS, international payment card fraud in 2006 was £117 million, which increased to £207 million in 2007. Majority was from countries which did not yet migrated to chip based cards. Card details and PIN codes are stolen by compromised devices or some other techniques. With the data, a counterfeit copy of the card can be produced [1].

Magnetic card reader and card is cheap to produce, for this reason attempt to make counterfeit version is greater. Security of data is thus extremely crucial here to save the valuable information for going to wrong person.
Magnetic card readers designed for smart phones do not contain any security itself. The application associated with card reading should therefore be secured. The application, customer and his data should also be secured in context of confidentiality, integrity, availability, authorization, and non-repudiation.

EMV® chip card technology is considered more secured than magnetic stripe swipe-based technology. This paper has addressed security issues of magnetic stripe card-based mobile payment, and a research based guideline is provided to minimize those vulnerabilities and threats. It is a well-known fact that absolute security is a myth; but we can take our concerned measure to save our resources as much as we can and make lives of perpetrator harder. Though magnetic stripe technology is old technology in context to chip based technology but it is still being used, because of its inexpensive implementation cost. Security is thus a primary concern here, especially when it is involved with mPayment - where sensitive-data and money is related.

1.4 Methodology

The design-science paradigm has its roots in engineering and the sciences of the artificial (Simon 1996). This paradigm is a problem solving one. It creates innovations which talks about the ideas, practices and technical capabilities. This paradigm analyses a product about its design, implementation, management and effective and efficient accomplishment of information systems [2].

An extensive research work was performed to establish a design of security model that can be used by the magnetic stripe. Being a card with static data and no processing capabilities, it was hard to design an effective secured solution. Eventually a best possible design was established considering the limitations. Based on the finding of the thesis, an application was built which is prototype and works with certain security features of the proposed solution. After the functional implementation feedback was taken from students and academic supervisors. The prototype was tested and some bugs were found and also it came to notice that certain features are needed to be improved. According to feedback it was further improved, both in term of interface and functionalities unless satisfactory performance was achieved.

![Figure 1: Reasoning in the design cycle [2]]
This paper is not a quantitative methodology as it is not involved in proving or disproving a hypothesis. This is not also a qualitative one, because the approach is not to produce several ideas that will produce one of more hypotheses for further testing. This is about designing artefacts and building an efficient and effective security solution for a product considering its technical capabilities.

1.5 Scope and Limitations

Due to time constraint, several interesting area were out of scope for performing research. This research focuses on the security of magnetic stripe-based mobile applications. After the swiping of the card, the communication security of user-data before it leaves the mobile terminal is within the scope of this research. Security of other components, such as card reader or card, security of over the air (OTA) is beyond the scope of this thesis work. Due to the lack of time, the application developing platform was for Android only, tested from version 2 to version 4. But the application developed does not work with few portable devices that runs on Android, for example, Samsung Galaxy Tab 2 is not supported; due to time limitation it was not taken into concern.

1.6 Structure of The Report

Chapter 1, Introduction: This Chapter discusses evolution of the mobile payment industry, obstacles in the growth of mobile payment market and solution, problem statement and research methodology.

Chapter 2, Transaction and Security: This chapter gives a brief overview of magnetic card technology and how it works. A brief discussion on the transaction pattern, important steps related to transaction, prime security terminologies are provided in this chapter.

Chapter 3, EMV Standard: A detailed discussion on EMV protocol has been discussed here. The overall security structure which is making EMV secured is discussed here.

Chapter 4, Overview of Security Services: This chapter discusses about PKI of different platforms.

Chapter 5, Securing Magnetic Stripe Card-Data Based on EMV Standard: This chapter outlines and describes the designed solution for mobile payment security vulnerabilities. The designs followed EMV standard. The design is evaluated for any breaches or vulnerabilities. To check the design practicality, a prototype has been developed; this chapter also describes about the prototype.

Chapter 6, Conclusion and Future Works: This chapter discusses the conclusion and some suggestion for future works are stated.
Chapter 2: Transactions and Security

2.1 Magnetic Stripe Cards

What are magnetic stripes? How do they work? A brief overview on magstripes technology would provide an understanding how the data the read and encoded. The elements of magnetic stripe are made of ferromagnetic materials. Ferro magnets are temporary magnets; it loses its magnetic property if an external magnetic source is removed. The bar that we see in the magnetic stripe card consists of elemental magnetic particle. Different types of cards have different density of magnetic stripe. These are defined by coercivity.

Coercivity is the intensity of magnetic field required to demagnetize a ferromagnetic material. Measuring unit is Oe and High energy magstripes and Low energy magstripes has the difference of 4000Oe and 300 Oe respectively. Low energy magstripes can easily be demagnetized if kept close to magnetic materials. High energy magstripes are more resistant to irrelevant magnetic fields. Inside the reader is semi-circular solenoid with concentrated permanent magnet at the edge of the face is situated. When the card is swiped, a reverse current in the solenoid causes flux reversal. South-South reverse flux created at rear edge of solenoid as can be seen in Figure 2.

<<<<<-Stripe movement direction

Figure 2: Reverse Flux Creation at Trailing Border [2]

Encoded magstripes are nothing but a collection of reverse flux fields. Hence the pattern will be like pole-like pole (NN, SS, NN). These inverse fluxes create the desired data. There is another solenoid called a Read Head, whose purpose is to detect the flux change. These are processed to produce encoded data. Different formation of magnetic pigments produce different encoding from the same reader.
As can be seen in the above Figure 3, the frequency of “1” bit is double than “0”. The actual data frequency depends on several factors, like the swipe speed, density of data etc. “1” will always have double frequency than “0”. There are two standards adopted for representing the binary data. One is ANSI/ISO BCD Data format and another is ANSI/ISO BCD Alpha format.

ANSI/ISO BCD Data format is a 5-bit binary coded decimal format. It has 16 characters’ set. The fifth bit is Odd parity bit which makes the entire bit to become odd.

At Figure 4, the left most bit (b1) is the least significant bit that is read first. Start Sentinel and End Sentinel tell the process of reformatting where to start grouping the decoded bit stream and where to stop followed by LRC. LRC is longitudinal redundancy check the parity check for all b1 to b4 data bits. It can fix errors such as error in two bits which could bypass parity check.
The second type of standard ANSI/ISO ALPHA Data Format can encode alpha numeric data. It involves 64 characters in seven bit character set. The last bit is also parity bit as before.

The data is stored in the tracks. There are three tracks in a magnetic stripe as defined by the ISO/ANSI. Tracks are identified based on their location in the homogenously magnetized card.

The 1st track is known as IATA (International Air Transport Association). One of its popular uses was ticket reservation where the customer information popped up in the display machines. This track contains customer name, account number and some other data. It follows the following format as in Table 1.

Table 1: Format and Description of Track 1 [33].

<table>
<thead>
<tr>
<th>Data</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start sentinel</td>
<td>1 byte (%)</td>
</tr>
<tr>
<td>Format code</td>
<td>1 byte alpha</td>
</tr>
<tr>
<td>Primary Account number</td>
<td>Up to 19 characters..</td>
</tr>
<tr>
<td>Separator</td>
<td>1 byte (^)</td>
</tr>
<tr>
<td>Country code</td>
<td>3 bytes (conditional)</td>
</tr>
<tr>
<td>Surname</td>
<td></td>
</tr>
<tr>
<td>Surname separator</td>
<td>(/)</td>
</tr>
<tr>
<td>First name or initial</td>
<td></td>
</tr>
<tr>
<td>Space</td>
<td>(when multiple data is present)</td>
</tr>
<tr>
<td>Middle name or initial</td>
<td>(when a title is there)</td>
</tr>
<tr>
<td>Period</td>
<td></td>
</tr>
<tr>
<td>Title</td>
<td></td>
</tr>
<tr>
<td>Separator</td>
<td>1 byte (^)</td>
</tr>
<tr>
<td>Expiration date or separator</td>
<td>4 bytes (YYMM) or the one byte separator if a non-expiring card.</td>
</tr>
<tr>
<td>Discretionary data</td>
<td>kept for Issuer’s use.</td>
</tr>
<tr>
<td>End Sentinel</td>
<td>1 byte (?)</td>
</tr>
</tbody>
</table>

The 2nd track is designed especially for banking activities. American Banking Association (ABA) has designed the specification for this track. It can be used in ATM, credit card checkers etc. It consists of information like cardholder’s account, encrypted PIN and some other related data. It follows the following format as in Table 2.

Table 2: Format and Data of Track 2 [33]

<table>
<thead>
<tr>
<th>Data</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start sentinel</td>
<td>1 byte (0x0B, or a ; in ASCII)</td>
</tr>
<tr>
<td>Primary Account Number</td>
<td>Up to 19 bytes</td>
</tr>
<tr>
<td>Separator</td>
<td>1 byte (0x0D, or an = in ASCII)</td>
</tr>
<tr>
<td>Country code</td>
<td>3 bytes (conditional)</td>
</tr>
<tr>
<td>Expiration date or separator</td>
<td>4 bytes (YYMM) or one byte separator if a non-expiring card.</td>
</tr>
<tr>
<td>Discretionary data</td>
<td>Kept for Issuer’s use.</td>
</tr>
<tr>
<td>End Sentinel</td>
<td>1 byte (0x0F, or a ? in ASCII)</td>
</tr>
<tr>
<td>Longitudinal Redundancy Check (LRC)</td>
<td>1 byte</td>
</tr>
</tbody>
</table>
The 3rd track is pretty much unused. Intention was to build a write enabled cared where information can be stored, for example it was a useful concept for offline ATM banking. But now most of the ATMs are online. Most of the readers are supports up to track 2. There is no specific standardization; hence as there is no uniform standard and guidelines for this track, it remained unused for mass commercial purpose [33].

2.1.1 Transaction flow of credit & debit card.

![Credit Card Transaction Diagram](image)

**Figure 5:** Credit Card Transaction [25]

The above Figure describes a credit/debit card transaction details. This transaction is similar for both swipe and chip based card. When the customer swipes or inserts the card in the reader, software attached with the reader at the point of sale (POS) of merchant terminal initializes a connection to the acquirer. Usually the track 2 contains the necessary data for such scenario; information includes, valid Account Number, Expiration date, Credit card limit and Card usage etc.

The Acquirer can be a bank or an organization whose task is to check the authenticity and validity of the request. The Acquirer sends request to the Issuer bank (responsible for customer’s payment) for checking the authorization of customer. If authorized, then the settlement of payment is performed. Getting the acknowledgement that customer is authenticated and authorized to pay the required money, merchant delivers the product and sends the info to Acquirer which deals the payment settlement with Issuer Bank. Upon the deduction of money the customer is acknowledged by Issuer that money is debited or credited from his account.

2.1.2 Security Vulnerabilities of Magnetic Stripe

The advantages of magnetic stripes are ease of encoding, cheap production costs, flexible portability also becomes the threat to clone the cards easily. All what is required is the access of the magnetic card for a while. Software and hardware equipment are available in market. Once successfully cloned, all securities are exploited.
2.2 EMV Transaction

EMV® is maintained by EMVco which manages, maintains and enhances the chip-based card specification for its interoperability with reading devices, such as ATM or Point of sales (POS). This chip-based card is known as EMV (Europay, MasterCard, and Visa), named after those developed it. EMV card contains a microprocessor chip which is capable of performing secured transaction at the POS.

The Terminal determines whether it is a chip based EMV card or magnetic stripe card. If the chip is read successfully then the transaction process starts. The processes described below shows the primary processes of EMV transactions. Details of the security related processes are discussed in security part of EMV in later chapter.

**Initiate Application**

Initiate Application: Inserting a card in the reader starts the initiation of transaction. The card is powered up and terminal expects an Answer to Reset (ATR) from card. ATR is a byte-
string which contains necessary information about the card, to set up the communication between terminal and card, this information is necessary. Initial put down of power and later turning on is called cold reset; which is takes place during initial start. There is another reset, warm reset, where terminal request the card a reset signal (without turning off the power) [19]. The merchant terminal contains a list of Application Identifier (AID). Every AID has

<table>
<thead>
<tr>
<th>Card scheme</th>
<th>RID</th>
<th>Product</th>
<th>PIX</th>
<th>AID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Visa</td>
<td>A0000000003</td>
<td>Visa credit or debit</td>
<td>1010</td>
<td>A00000000031010</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Visa Electron</td>
<td>2010</td>
<td>A00000000032010</td>
</tr>
<tr>
<td></td>
<td></td>
<td>V PAY</td>
<td>2020</td>
<td>A00000000032020</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Plus</td>
<td>8010</td>
<td>A00000000038010</td>
</tr>
<tr>
<td>MasterCard</td>
<td>A0000000004</td>
<td>MasterCard credit or debit</td>
<td>1010</td>
<td>A00000000041010</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MasterCard</td>
<td>9999</td>
<td>A00000000049999</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Maestro (debit card)</td>
<td>3060</td>
<td>A00000000043060</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cirrus (interbank network)</td>
<td>6000</td>
<td>A00000000046000</td>
</tr>
<tr>
<td>UK Domestic Maestro - Switch (debit card)</td>
<td>A0000000005</td>
<td>Maestro UK</td>
<td>0001</td>
<td>A00000000050001</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Solo</td>
<td>0002</td>
<td>A00000000050002</td>
</tr>
<tr>
<td>American Express</td>
<td>A0000000025</td>
<td>American Express</td>
<td>01</td>
<td>A0000000002501</td>
</tr>
<tr>
<td>RuPay (India)</td>
<td>A0000000024</td>
<td>RuPay</td>
<td>1010</td>
<td>A00000000241010</td>
</tr>
<tr>
<td>Discover</td>
<td>A0000000152</td>
<td>Discover</td>
<td>3010</td>
<td>A00000001523010</td>
</tr>
<tr>
<td>Interac (Canada)</td>
<td>A0000000277</td>
<td>Debit card</td>
<td>1010</td>
<td>A00000002771010</td>
</tr>
<tr>
<td>JCB</td>
<td>A0000000065</td>
<td>Japan Credit Bureau</td>
<td>1010</td>
<td>A00000000651010</td>
</tr>
<tr>
<td>LINK (UK) ATM network</td>
<td>A0000000029</td>
<td>ATM card</td>
<td>1010</td>
<td>A00000000291010</td>
</tr>
<tr>
<td>Dankort (Denmark)</td>
<td>A0000000121</td>
<td>Debit card</td>
<td>1010</td>
<td>A00000001211010</td>
</tr>
</tbody>
</table>

Figure 7: AID and Corresponding Card Schemes [34]

specific card associated algorithm and parameter which determines the way of transaction processing. At least one application ID should match between the card and the terminal. Both have a number of AIDs. If they do not match, then according to policy of the merchant, it will be determined whether transaction will be processed or terminated. [8].

If the AID matches then the terminal selects the application on payment card for correct data transfer. Upon getting get processing option command from card, the chip of the payment Card provides the AFL (application file locator). AFL contains useful data records for the terminal to understand which part of data is for authentication, which is for transaction etc.

Read Application Data

Chip contains files and records, pointed at AFL, which has the EMV data such as card holder verification, card authentication, and expiry date etc. that are required for transactions. In order to keep the transaction flow going, the terminal must be able to read the files. Files are read by the command Read Record [9].

Offline Data Authentication

This is carried offline thus it is never used in online data authentication like ATM. Terminals providing EMV services have to provide any one of the following services: Static Data
Authentication (SDA), Dynamic Data Authentication (DDA), Combined DDA and Application Cryptogram Generation (CDA). If the ICC and Terminal both support CDA, then, CDA will be performed. If ICC and Terminal both support DDA, then, DDA will be performed. Otherwise if both support SDA, then, Static Data Authentication will take place. In order to perform successful Offline Data Authentication, both ICC and Terminal should support a common authentication method, if none matches then no offline authentication will take place. The offline methods are discussed later [26][9].

**Process Restriction**

Compatibility between the applications of the Terminal and ICC is checked in Process Restrictions. Necessary adjustments or if adjustment fails then possible rejection is done in this step. The time validity is checked in this step. Application version number, Application Usage Control and Expiry date are the three elements which are checked. Though the card is not instantly rejected if the expiry date is over, rather it is checked by Issuer whether they permit expired card for transaction. [26][9]

**Cardholder Verification**

Cardholder verification method (CVM) is used to find out if the card holder is the actual legitimate user. The Terminal has a list of CVM that it supports and condition of execution. If allowed, upon failing of one method it goes through the list according to the set priority, to execute another method. The ICC must support at least one of the CVM. Terminal recognizes and checks for compatibility. If recognized and supported, then CVM is performed. If CVM is unsuccessfully performed then it goes for next Cardholder Verification rules. CVM is considered failed if the last method of the CVM list fails processing or if any CVM cannot verify the cardholder [26][9].

The There are various types of CVM: Signature, Offline plaintext PIN, Offline enciphered PIN, Offline plaintext PIN and signature, Offline enciphered PIN and signature, Online PIN, No CVM required and Fail CVM processing (detail discussion on CVM can be found later).

**Terminal Risk Management**

Terminal Risk Management is measure to keep the customer, merchant, acquirer and Issuer safe from fraud. For huge value transaction, Terminal Risk Management provides positive Issuer authorization and also takes transaction online sometimes, to avoid undetectable deception in offline mode.

TRM is not available where type of transaction, online or offline is permanently defined. It manages the risk of fraud by checking the transaction value range authorized to the card holder, if suspicious transaction was made previously, for example, too much offline transaction with same card etc. [9]

**Terminal Action Analysis**

It uses the result of the risk management steps, verification, authentication, and decides appropriate step, to shoot online or approve/disapprove offline output. If the terminal offers online transaction then the payment cannot be done by offline transaction [9].
Card Action Analysis

ICC has its own risk management system, which is Issuer specific. The risk management and corresponding card action protects the credit risk of the card and frauds. The ICC takes the decision based on the risk calculation whether the transaction will be online, offline or rejected. If offline transaction is approved, the ICC sends Transaction Certificate (TC) to the Issuer. Successful verification means payment is accepted. For the online transaction processing, ICC sends ARQC to Issuer.

The card generates ARQC which is a digital signature. When ARQC is requested the transaction goes online and Issuer checks the generated ARQC by the card. The Issuer responses with which says to allow or reject the transaction through authorization response cryptogram (ARPC) and a script processing starts to send command to ICC. If ARPC contains approval then TC is sent by ICC like in the Card Action Analysis. [26][9]

Online Processing

Online processing ensures that the transaction is within the defined acceptable limit. The Issuer reviews if the transaction is beyond the risk-limit, which is set earlier by Issuer or Acquirer or the payment system, and either decline or authorized the transaction. After the ICC is authenticated by the Issuer, it generates a cryptogram based on particular data in the authorization or shared data, and as a part of Issuer Authentication Data it is passed to the merchant-Terminal. Terminal puts this in the command EXTERNAL_AUTHENTICATION or secondly GENERATED_AC command. There are two ways by which ICC can response, EXRNAL_AUTHENTICATION command is used when Issuer recognizes that ICC is capable of Issuer authentication or ICC combines an Issuer authentication function with GENERATED_AC command. Successful online processing completes with Issuer authentication. [26][9]

Issuer-to-Card Scripting

Script command can be encrypted between card and the Issuer, that is, the Terminal will just be a deliverer in that case. Script is used to feed data to card or block the card or to perform other functions which may be irrelevant to current transaction. [26]

If the Issuer has authorized the payment and the card authenticated the received data, the terminal approves the payment and asks to remove the card. Goods can be collected from the merchant.

2.3 Security Basics

Data is the raw format of bit stream which is to be further processed. This is such stated because it is the prerequisite of information. It is mostly static. Data can be characterized as set of distinguishable facts about events. [13]

Message is a carrier which can carry data, information or knowledge. The data, information or knowledge are carried as message.

Information is the aggregated and processed data. It is completely meaningful and has a purpose. In contrast to data, information is not static. Decisions can be taken based on the information obtained.
Knowledge is the fine processing of information where appropriate study, analysis and experience is involved. Conjugation of fact, procedural rules and heuristics can also be key element of knowledge. Knowledge is about truth which is denoted by facts. Procedural rules talks about the action. Heuristic figures out a way to deal with a problem by studying the experiences on the subject matter [14].

Data when synchronized to desired pattern forms information. Processed information when bound with more study, analysis and includes extract of experience is knowledge. A message is a carrier, which can be encoded if wished. It carries data, information or knowledge from sender to receiver. Cognition is a platform for knowledge to be further analysed for more accuracy in its application.

**Threat**

Threat is a something which is under direct attack of intruders or attackers. It is rather the possible flaw in a system which is vulnerable to the security. For being a threat it is not something that the violation has already taken place.

Four broad classes [15] are stated by Shirey regarding threats,

**Disclosure:** Where an unwanted person can have unauthorized access to the system or information.

**Deception:** False information is accepted within the system.

**Disruption:** To hamper the correction operation from performing.

**Usurpation:** Partially take control of a system.

Defining security is an ambiguous effort. It depends on the context it is referring to. The trust and security in information technology context can be categorized into confidentiality, integrity, availability, authenticity and non-repudiation.

Confidentiality prevents the data to be exposed to others except the desired person. The concealment of data or information is a prevention to keep the attacker unaware of its existence. Section 1.1[15]

In mobile payment only two bodies should be concerned about the data: the chip card which is generating cryptogram and the server (can be acquirer's server for example) which is decrypting.

Integrity is the confirmation that data is not tampered. Integrity is not for data only, but also applicable to source or origin. Unaltered data, if imported from a source, which provided wrong information leads to a security breach. Section 1.1[15]

For mobile payment, it is important from the first stage to the last; that from the data that belong to customer to should be transmitted to terminal from the chip in unaltered form, till the Issuer sending money deduction message.

Availability is a main aspect of security. All the security and safety is taken so the subject is accessible. While designing a system, it is very crucial to keep the backup system equally secured. This is because a perpetrator can compromise the secondary system first, and then make the main system inaccessible to others (eg. By DoS attack) Section 1.1[15]
Though in the payment industry, the backup of data is not applicable at times. While payment transaction is live it is very crucial that no data is lost at any of the stages. Otherwise, the undesired incident can take place, like products not delivered to customer.

Identification and authentication seems to be very similar, but actually both are independent service dependent on one another. Identification is determined by system or network by recognizing one’s existence as an entity. To verify that identity is authentication, usually with the help of credentials like by providing PIN code through smart cards, identification through fingerprints etc.

Non-repudiation is the part of security entity where an involved party cannot deny his participation in a transaction that actually took place.

**2.3.1 Attacking through forcing to Fall-back**

Some of the data in the EMV chip is identical to the track-two data of the magnetic stripe. If the data between the card and terminal can be intercepted, then attacker can retrieve track two data and PIN - use those data to build a magnetic stripe card and put those data in it. The chip of the card can be tampered and made unusable in which case the terminal will ask to fall-back. Fall-back is the magnetic stripe service when chip-based card is not working. This is not possible in every terminal, but possible where the followings take place:

i) Offline PIN is in plaintext format.

ii) Fall-back to swipe card is allowed by merchant.

iii) Card Issuer does not consider the geographical & behavioural checking.

Most of the above cases are still valid where chip-based technology is not popular yet. [17]
Chapter 3: EMV Standard

Magnetic Stripe is fairly an old technology. Despite it is a cheap technology to implement it was never a secured one. Initially the manufacturing procedure of magnetic card and its reader were kept secret. Only some professional bodies and certain manufacturers possessed the blueprint of this technology. But as time has flowed the procedure and design was revealed or found out. As it is a cheap technology, faking a card and fraud gradually increased over time. There are more secured payment solutions present in the market now a days, one of the most promising technology being EMV as discussed in the previous chapters.

3.1 Why Magnetic Stripe-based Solution?

In one word, it is yet one of the most popular technologies for transactions. That is why in most of the PoS, even where EMV payment is accepted, usually keeps a backup plan (often known as Fall-back) to use magstripes if EMV transactions fails or not supported. Some of the medium developed and most of the underdeveloped country still use magnetic stripe based solution, because it is cheaper to implement and maintain. It is prominent that at one stage most of the POS will be using EMV or similar secured technology. But considering the number of exiting countries using magstripes, a good deal of time should be needed for full migration towards the more secure technology. Till then what will happen to customers using magnetic stripes? Payment Card Industry Data Security Standard. (PCI DSS) is a body which is trying to prevent fraud and attacks on magnetic stripes based payments. Their main concern is to secure the merchant terminal to resist the attack. But, the principal problem being not to protect the card data itself, the chance of duplicating the card still remains. [18]

There should be some approach which will protect the customer side. By that it is meant that the card data should be protected. Even if it goes to wrong hand, the attacker should not be able to use that card by impersonating as a genuine customer.

The security solution for the Magnetic Stripe provided in this paper is a solution for mobile based payment. To be more specific, it is a solution for smart phone based technology. Beside the traditional POS, smart phone based payment became a popular mode of transaction because of the several reasons which is described in Chapter 1. But, there are always risks while playing with data, especially when it is regarding payment, so highest priority should be given, to make the entire payment secured.

But, as mentioned earlier, here the merchant’s device is the more secured one. But the security of customer is also considered unlike, PCI DSS. If the customer loses the card somehow and it goes to wrong hand, even then he cannot use the card. Attacker will have the card but not the PIN which will be issued separately to the customer. That PIN is not embedded the card.

Considering the security of customer and the merchant, this design aims to facilitate secured smart phone based transaction.
3.2 EMV Security

3.2.1 Card Authentication Method
The card needs to be authenticated and authorized in order to prevent the use of counterfeited and skimmed cards to take part in transaction.

3.2.1.1 Online Card Authentication
In an online card authentication, the transaction is sent online so that the Issuer can authenticate and authorize it [12]. This authentication and authorization is similar in a way for both magnetic stripe transaction and EMV transaction, both uses symmetric key in this purpose. But the dissimilarity is in the use of the symmetric key by the chip. In case of magnetic stripe, the symmetric key is static.

In case of ICC, its chip generates a dynamic data which is called ARQC (Authorization Request Cryptogram). The cryptogram is generated using a cryptographic algorithm utilizing the transaction data and card and terminal data. This using of several data makes the cryptogram unique. The algorithm can be any symmetric algorithm (defined before) like AES or Triple DES etc. EMV card has one key, which is securely stored in the chip. The other key is with Issuer. But the Issuer does not store the other key; using the Primary Account Number (PAN), it derives the key from a master key. Issuer can thus authorize and authenticate the card and transaction. [12]

3.2.1.2 Offline Card Authentication
In an Offline Card Authentication, connection to the Issuer is not required, prioritized; rather a chain-of-trust is established for authentication and verification. The concurrent participating bodies are EMV card and Terminal. Three types of Offline Card Authentication are:

- Static Data Authentication (SDA)
- Dynamic Data Authentication (DDA)
- Combined DDA with Application Cryptogram (CDA)

Below it is briefly described how the offline authentication is carried out:

**Static Data Authentication**
Static Data Authentication is used to prevent any modification or alteration of the card data. SDA is performed by the Terminal; it verifies the digital signature by verifying a pre-generated static signature saved in the chip, which is signed by Issuer’s private key.
This offline data is authenticated using public key infrastructure, based on the RSA algorithm to confirm legitimacy of the ICC-data.

**Figure 8: Offline Static Data Authentication [22]**

Static Application Data is signed by Si (the private key of the Issuer) and is kept as signed application data (SSAD). Public key of the Issuer is signed by the private key of Certificate authority (CA) to verify that it is actually the Issuer and stored in the card as Issuer PK certificate. These are provided by the card to terminal. The CA Public key is stored in IC Terminal (PCA). Through the PCA public key is extracted and verified successful decryption of Issuer PK certificate. With this public key it is verified if SSAD was signed by Issuer. Successful verification of SSAD means SDA succeeded. [22]

The counterfeiting and cloning problems are still unsolved with SDA. That means if a fake card with data cloned from the original card is provided; the terminal still shows successful SDA, even if the card is counterfeited.

**Dynamic Data Authentication**

As mentioned earlier, SDA cannot detect the counterfeited cards; offline Dynamic Data Authentication is a different scheme which can detect the cloned copy of cards. It also uses PKC to validate the legitimacy of stored or generated data of ICC and also the data got from the terminal.

Offline Dynamic Data Authentication is a secured authentication by utilizing public key signing method. Involving CA to sign the public keys makes it cryptographically a highly secured method. But for proper execution of this system, every terminal should store CA public key for each application [22].

In Figure 9, the Issuer public key certificate is PI is signed by CA (SCA)
Figure 9: Offline Dynamic Data Authentication [22].

Issuer PK certificate contains cryptographic information that Issuer Public Key(P1) is signed by CA (SCA). There are two new keys in this scenario, the private key of ICC (SIC) and the public key of ICC(SIC). Static Application Data and public key of ICC (PIC) is signed by the public key of Issuer (P1). The dynamic data is signed by the private key of card (SIC). In the terminal end, public key of CA is stored which is used to verify the Issuer’s Public Key (P1). With P1, static application data and the public key of ICC (PIC) is verified. PIC verifies the signature on the dynamic data.

**Combined DDA (CDA) with Application cryptogram.**

Combined DDA is an enhanced version of DDA. DDA could detect a counterfeited or cloned copy of card. But what if there is a wedge device placed in between card and terminal stealthily? DDA cannot thus prevent man in the middle attack. CDA is capable to detect the man-in-the-middle attack by verification of the signature by terminal using an Application Cryptogram (AC). CDA combines the application cryptogram and dynamic signature calculation in one command, which makes the process faster. CDA is recommended for contactless payment, as in contactless payment, DDA will decrease with overall performance because of its slow speed. But CDA is still new and not widely deployed yet. [22]

**3.2.2 Card Holder Verification Method**

Cardholder Verification Method (CVM) is performed to authenticate that legitimate user is using the card to whom the card application has been issued. If the Application Interchange Profile is set to bit 1, then CVM will be performed. The terminal goes through the CVM list in the chip which is put in order. If there is no CVM list present in the chip then verification process is terminated. [26]

The CVM list is an object with composite data of Amount field, second Amount field and Customer verification rules (CV rules). Table 3 shows the list.
Table 3: CVM Codes and Methods [26]

<table>
<thead>
<tr>
<th>CVM List</th>
<th>b8</th>
<th>b7</th>
<th>b6</th>
<th>b5</th>
<th>b4</th>
<th>b3</th>
<th>b2</th>
<th>b1</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Fail CVM processing</td>
<td>Reserve</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>2. Plaintext PIN verification</td>
<td>Reserve</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>3. Enciphered online PIN verification</td>
<td>Reserve</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>4. Plaintext PIN verification and Signature verification</td>
<td>Reserve</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>5. Enciphered offline PIN verification</td>
<td>Reserve</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>6. Encipher PIN verification and Signature verification</td>
<td>Reserve</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>7. Signature verification</td>
<td>Reserve</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>8. No CVM needed</td>
<td>Reserve</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
</tbody>
</table>

There are eight types of CVM [23]. Depending on the CVM supported by both ICC and terminal verification is performed.

**Enciphered offline PIN Verification:** The PIN provided by user is encrypted-decrypted using asynchronous encryption(RSA) by terminal and ICC. Both must be capable to handle RSA type encryption. After decryption by ICC it checks the reference in its internal memory.

**Plain Text offline PIN Verification:** A PIN is taken from the user and without any encryption it is passed to ICC. Then the provided PIN is compared with the one stored in the ICC chip memory.

**Plain text offline PIN & Signature Verification.** This is a combined verification which performs both plain text offline verification and signature verification (described below).

**Enciphered offline PIN & Signature Verification:** This is a combination verification which performs both enciphered offline PIN verification and signature verification.

**Online Enciphered PIN Verification.** Terminal encrypts the PIN that it gets from the user and sends it to Issuer's network for verification.

**Signature Verification:** This is one of the very primitive methods of verification; it uses a paper at which the user signs, merchant checks if provided signature matches the signature signed in the back of the card.

**NO CVM:** This option is kept for quick and fluent transaction. Security is almost none here. It is not verified whether possessor of the card is its real owner.
3.2.3 Key Management

For supporting the SDA feature, the ICC must have the elements mentioned in the Table 4 [22]. Each terminal must store six CA public keys per RID(Registered Application Provider Identifier) and shall be able to use the key in association with the key and key regarding information. Terminal must be capable of locating the associated key with CA public key index the RID provided. Table 4 shows required data elements for SDA.

<table>
<thead>
<tr>
<th>Required Data Elements</th>
<th>Length</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certification Authority Public Key Index</td>
<td>1</td>
<td>Finds out CA Public Key of the application and corresponding algorithm should be used with chip.</td>
</tr>
<tr>
<td>Issuer Public Key Certificate</td>
<td>var.</td>
<td>Card Issuer gets this from CA. Terminal verifies this element and then Issuer Public Key is authenticated.</td>
</tr>
<tr>
<td>Signed Static Application Data</td>
<td>var.</td>
<td>This digital signature is generated by Issuer, by signing with its Private Key.</td>
</tr>
<tr>
<td>Issuer Public Key Remainder</td>
<td>var.</td>
<td>The presence of this data element in the chip</td>
</tr>
<tr>
<td>Issuer Public Key Exponent</td>
<td>var.</td>
<td>Provided by the Issuer.</td>
</tr>
</tbody>
</table>

Overview of Keys and Certificates

For SDA to work, Signed Static Application Data, signed using the private key of Issuer, should be stored in the ICC. ICC should also have the public key of the Issuer along with the public key certificate.

There are three major steps that involve key and certification process, used in SDA, as Specified in [22].

- The Terminal retrieves Certification Authority Public Key.
- The Terminal retrieves Issuer Public Key.
- The Terminal verifies Signed Static Application Data.
Key Management in DDA (Dynamic Data Authentication)

While most of Static Data Authentication is still widely used, the future of Dynamic Data Authentication (DDA) is more prospective, because it provides more security than SDA. SDA authenticates a single signature every time. DDA on the other hand authenticates new signature each time. DDA chip is contains a crypto processor which can generate data that allow verification of card holder, risk management and authentication offline. DDA can, as having computational capability can have its own key pair to compute and encrypt the PIN of the card.

The security of DDA is supported by certification authority, an extensive cryptographic facility which signs the public keys. For the offline DDA, each application recognized by terminal should have corresponding public key of CA. ICC contains the following elements to support the offline DDA.

<table>
<thead>
<tr>
<th>Required Data Object</th>
<th>Length</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certification Authority Public Key Index</td>
<td>1</td>
<td>Finds out CA Public Key of the application and corresponding algorithm should be used with chip.</td>
</tr>
<tr>
<td>Issuer Public Key Certificate</td>
<td>var.</td>
<td>Card Issuer gets this from CA. Terminal verifies this element and then Issuer Public Key is authenticated.</td>
</tr>
<tr>
<td>ICC Public Key Certificate</td>
<td>var.</td>
<td>ICC gets this from Issuer; terminal verifies the element and authenticates the Public Key of ICC.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Required Data Object</th>
<th>Length</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Issuer Public Key Remainder</td>
<td>var.</td>
<td>Described later</td>
</tr>
<tr>
<td>Issuer Public Key Exponent</td>
<td>var.</td>
<td>Provided by the Issuer</td>
</tr>
<tr>
<td>ICC Public Key Remainder</td>
<td>var.</td>
<td>Described later</td>
</tr>
<tr>
<td>ICC Public Key Exponent</td>
<td>var.</td>
<td>Provided by the Issuer</td>
</tr>
<tr>
<td>ICC Private Key</td>
<td>var.</td>
<td>Remains secret in ICC. Used to generate the Signed Dynamic Application Data.</td>
</tr>
<tr>
<td>Signed Dynamic Application Data</td>
<td>var</td>
<td>It is generated by the chip using its private key. It is a digital signature containing critical data elements from ICC and Terminal.</td>
</tr>
</tbody>
</table>
There are certain requirements for the terminal that supports Offline DDA. As mentioned above, it should have computational ability. Besides, it should be able to store six Certification Authority (CA) Public Keys per RID (Registered Application Provider Identifier). The terminal should be capable to find the key based on RID and CA public key index [22].

The initial steps taken by Terminal in the process of offline authentication are [22]:

- Terminal retrieves Public Key of CA
- Terminal retrieves Public Key of Issuer
- Terminal retrieves ICC Public Key.

**Certificates and Keys**

ICC has a pair of keys (Public and Private Keys) for securing offline Dynamic Data Authentication. The public key of ICC is placed in ICC as a public key certificate. The three-layer public key certification system secures the offline DDA. Terminal goes through two levels verification of certificates to get and verify the public key of ICC. After retrieving of that ICC public key it can verify the dynamic signature of ICC. Key modulus and exponent sizes are the following [22]:

Leftmost bit of left most byte is 1 and the bit length of moduli will be multiple of 8. Public key modulus of CA is $N_{CA}$ bytes, then $N_{CA}\leq 248$. The public key exponent of CA $\geq 3$ or $2^{16} + 1$.

Public key of modulus of public key pair of Issuer is $N_I$ bytes, where $N_I \leq N_{XA} \leq 248$. If $N_I > (N_{CA} - 36)$, the Public Key Modulus of Issuer will have one segment containing the most significant bytes of the modulus (of the $N_{CA} - 36$) and another part is the least significant bytes of the modulus consisting of the remaining. The Issuer Public Key Exponent is $\geq 3$ or $2^{16} + 1$.

Public key of modulus of public key pair of ICC is $N_{IC}$ bytes, where $N_{IC} \leq N_I \leq N_{CA} \leq 248$. If the $N_{IC} > (N_I - 42)$, the Public Key Modulus of the Issuer will have one segment containing the most significant bytes of the modulus (of the $N_{CA} - 42$) and another part is the least significant bytes of the modulus consisting of the remaining. The Issuer Public Key Exponent is $\geq 3$ or $2^{16} + 1$.

For successful operation of offline DDA public key, the authentication has to be successful. The terminal fetches and authenticates the public key of ICC. The following information can be fetched by using READS RECORD command except the RID. RID can be obtained from AID [22]. Table 6 shows data objects required for DDA.
Table 6: Data Objects Required for Offline DDA [22].

<table>
<thead>
<tr>
<th>Tag</th>
<th>Length</th>
<th>Value</th>
<th>Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>—</td>
<td>5</td>
<td>Registered Application Provider Identifier (RID)</td>
<td>b</td>
</tr>
<tr>
<td>'8F'</td>
<td>1</td>
<td>Certification Authority Public Key Index</td>
<td>b</td>
</tr>
<tr>
<td>'90'</td>
<td>N&lt;sub&gt;CA&lt;/sub&gt;</td>
<td>Issuer Public Key Certificate</td>
<td>b</td>
</tr>
<tr>
<td>'92'</td>
<td>N&lt;sub&gt;L&lt;/sub&gt; - N&lt;sub&gt;CA&lt;/sub&gt; + 36</td>
<td>Issuer Public Key Remainder, if present</td>
<td>b</td>
</tr>
<tr>
<td>'9F32'</td>
<td>1 or 3</td>
<td>Issuer Public Key Exponent</td>
<td>b</td>
</tr>
<tr>
<td>'9F46'</td>
<td>N&lt;sub&gt;L&lt;/sub&gt;</td>
<td>ICC Public Key Certificate</td>
<td>b</td>
</tr>
<tr>
<td>'9F48'</td>
<td>N&lt;sub&gt;IC&lt;/sub&gt; - N&lt;sub&gt;L&lt;/sub&gt; + 42</td>
<td>ICC Public Key Remainder, if present</td>
<td>b</td>
</tr>
<tr>
<td>'9F47'</td>
<td>1 or 3</td>
<td>ICC Public Key Exponent</td>
<td>b</td>
</tr>
<tr>
<td>—</td>
<td>Var.</td>
<td>Static data to be authenticated as specified in section 10.3 of Book 3 (see also section 6.1.1)</td>
<td>—</td>
</tr>
</tbody>
</table>

Certification Revocation List

If the terminal supports Certification Revocation List (CRL), it can check, whether the RID, CA public key index, and the certificate’s serial number obtained from Issuer’s public key certificate is in the revocation list. If it is, then the DDA fails.

Retrieval of The CA Public Key

The terminal reads the CA public key index. Using this index and RID, the terminal reads CA public key modulus, key and related information and matching algorithm that resided in the terminal. If the key index and RID mismatch with the stored key, then offline DDA fails.

Retrieval of the Issuer public Key

CA public key modulus and Issuer’s public key index should be of the same of same length. For successful offline DDA accomplishment, following conditions have to be true [22]:

- Recovery function on Issuer public key certificate should bring the Recovered Data Trailer equivalent to “BC”.
- Recovered Data Header should be “6A”.
- Certificate format should be “02”.
- Proper concatenation for certification format
- To the result of concatenation, the hash algorithm should be properly inserter to produce the hash result.
- Successful comparison between calculated hash result and derived hash result.
• Left most 3-8 PAN digit should match Issuer Identifier.
• The expiry date of certificate is equal or more than current date, i.e. expiry date has not expired yet.
• Valid concatenation of Certificate serial number, Public Key index and concatenation of RID.
• Issuer Public Key Algorithm Indicator must be recognized.

After successful completion of the above procedures, the leftmost digit of the Issuer’s Public Key, if present, the Issuer’s public key remainder are concatenated to find out the Issuer Public Key Modulus. This Issuer Public Key Modulus will be used for retrieving the public key of the chip.

Table 7: Recovered Data Format from Issuer PKC [22]

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Length</th>
<th>Description</th>
<th>Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recovered Data Header</td>
<td>1</td>
<td>Hex value '6A'</td>
<td>b</td>
</tr>
<tr>
<td>Certificate Format</td>
<td>1</td>
<td>Hex value '02'</td>
<td>b</td>
</tr>
<tr>
<td>Issuer Identifier</td>
<td>4</td>
<td>Leftmost 3-8 digits from the PAN (padded to the right with Hex 'F's)</td>
<td>cn 8</td>
</tr>
<tr>
<td>Certificate Expiration Date</td>
<td>2</td>
<td>MMYY after which this certificate is invalid</td>
<td>n 4</td>
</tr>
<tr>
<td>Certificate Serial Number</td>
<td>3</td>
<td>Binary number unique to this certificate assigned by the certification authority</td>
<td>b</td>
</tr>
<tr>
<td>Hash Algorithm Indicator</td>
<td>1</td>
<td>Identifies the hash algorithm used to produce the Hash</td>
<td>b</td>
</tr>
<tr>
<td>Issuer Public Key Algorithm Indicator</td>
<td>1</td>
<td>Result in the digital signature scheme</td>
<td>b</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Identifies the digital signature algorithm to be used with the Issuer Public Key</td>
<td></td>
</tr>
</tbody>
</table>

Table 7: Recovered Data Format from Issuer PKC [22]

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Length</th>
<th>Description</th>
<th>Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>Issuer Public Key Length</td>
<td>1</td>
<td>Identifies the length of the Issuer Public Key Modulus in bytes</td>
<td>b</td>
</tr>
<tr>
<td>Issuer Public Key Exponent Length</td>
<td>1</td>
<td>Identifies the length of the Issuer Public Key Exponent in bytes</td>
<td>b</td>
</tr>
<tr>
<td>Issuer Public Key or Leftmost Digits of the Issuer Public Key</td>
<td>NCA – 36</td>
<td>If NI ≤ NCA – 36, consists of the full Issuer Public Key padded to the right with NCA – 36 – NI bytes of value 'BB'</td>
<td>b</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If NI &gt; NCA – 36, consists of</td>
<td></td>
</tr>
</tbody>
</table>
the NCA – 36 most significant bytes of the Issuer Public Key

<table>
<thead>
<tr>
<th>Hash Result</th>
<th>Hash of the Issuer Public Key and its related information</th>
<th>b</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recovered Data Trailer</td>
<td>Hex value 'BC'</td>
<td>b</td>
</tr>
</tbody>
</table>

**Retrieval of The ICC Public Key**

Issuer’s public key modulus and ICC public key certificate should be same of the same length. For successful offline DDA accomplishment, several conditions have to be true [22].

- Recovery function on ICC public key certificate should bring the Recovered Data Trailer equivalent to hexadecimal value “BC”.
- Recovered Data Header should be “6A”.
- Certificate format should be “04”.
- Proper concatenation for certification format.
- To the result of concatenation, the indicated hash algorithm should be properly inserted to produce the hash result.
- Successful comparison between calculated hash result and derived hash result.
- Application PAN that is read from ICC and recovered PAN comparison should match.
- The expiry date of certificate is equal or more than current date, i.e. expiry date has not expired yet.
- Valid concatenation of Certificate serial number, Public Key index and concatenation of RID.
- ICC Public Key Algorithm Indicator must be recognized.

After the successful completion of the above procedures, the left most digit of ICC public key and if present, the ICC public key remainder is concatenated to find out the ICC Public Key Modulus. This ICC Public Key Modulus will be used for Offline DDA.

**Dynamic Signature Generation**

For Dynamic Signature Generation, a command (INTERNAL AUTHENTICATE) and some data element is issued by Terminal, specified by DDOL (Dynamic Data Authentication Data Object List). DDOL has object list that contains length and tag data, which is fed into INTERNAL AUTHENTICATE that is passed to ICC. It is optional for ICC to contain DDOL, but the terminal must have DDOL.

The following conditions must be true for successful Offline DDA [22].

A. Terminal and ICC (optional) have DDOL.
B. DDOL of the terminal or ICC contains unpredictable number
C. DDOL and unpredictable number, these both cannot be absent at both terminal and ICC.

Table 8: Dynamic Application Data to be Signed [22]

<table>
<thead>
<tr>
<th>Description</th>
<th>Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signed Data Format</td>
<td>Hex value '05'</td>
</tr>
<tr>
<td>Hash Algorithm Indicator</td>
<td>Identifies the hash algorithm used to produce the Hash Result</td>
</tr>
<tr>
<td>ICC Dynamic Data Length</td>
<td>Identifies the length L_{DD} of the ICC Dynamic Data in bytes</td>
</tr>
<tr>
<td>ICC Dynamic Data</td>
<td>Dynamic data generated by and/or stored in the ICC</td>
</tr>
<tr>
<td>Pad Pattern</td>
<td>(N_{IC} – L_{DD} – 25) padding bytes of value 'BB'</td>
</tr>
<tr>
<td>Terminal Dynamic Data</td>
<td>Concatenation of the data elements specified by the DDOL</td>
</tr>
</tbody>
</table>

ICC creates the dynamic digital signature with ICC’s private key and specified algorithm, which is called Signed Dynamic Application Data.

3.2.4 EMV Offline Transactions Risk Management

Terminal risk management is a protection scheme. The terminal performs it to protect the system, Issuer and Acquirer by using several techniques desriber later. ICC has to go online for this protection to work, because in offline environment threats might be there undetected. This risk management is initiated if the "terminal risk management is to be performed" bit is set to 1 in the Application Interchange profile. This management is performed before Generate AC command is issued, and after Read Application Data.

Three types of management are discussed below [26] which protect the system, Issuer and Acquirer are:

- Floor limit checking
- Random transaction selection
- Velocity checking.

Successful completion of the management is shown by putting "Terminal risk management was performed" bit to 1.

Floor Limit

Floor Limit is the boundary of the payment scope of payee. If the terminal is capable of checking floor limit, transaction outside the floor limit will not be processed. It also deals with split a sale that is paying through several times by one account. Floor limit can prevent split
sales by not allowing the total authorized sum of money allowed to be exceeded. Some terminals can store log file of an Application PAN, its sequence number and transaction date. Through the log it is determined if the sum of transaction exceeds the limit allocated. If it is equivalent or more than terminal floor limit then "Transaction floor limit" is set to 1. If the log is unavailable or blank under same PAN, then the amount is checked with the floor limit to decide whether transaction will be processed.

**Random Transaction Selection**

Beside floor limit, there are specifications by applications

a. Target percentage from 0 to 99% should be used for Random Selection

b. Threshold value, in between 0 or +ve number < Floor Limit, specified for Biased Random Selection.

c. Maximum Target Percentage should be at least equivalent to highest value of Target Percentage( between 0% and 99%). It is required for Biased Random Number

**Velocity Checking.**

Velocity Checking is processing a transaction online after certain number of offline transaction. Lower consecutive Offline Limit is the soft cap, which if written requires next transaction to go online. If online is unavailable, then it is processed offline as usual. Upper Consecutive offline limit sets the hard cap which makes transaction through online mandatory. There are two more objects, Application Transaction Counter (ATC) and Last Online ATC Register. The difference between these two tells about the limit. Unavailability of Lower and Upper Offline-limit data object in the ICC makes the terminal skip the velocity checking.
Chapter 4: Overview of Security Services in Mobile Environments

4.1 PKI Overview

A PKI [27] stands for Public Key Infrastructure. It is a set of several entities which uses public key cryptography and certificate management for security. A PKI is apparently capable for providing the pillars of security: confidentiality, integrity, authentication and non-repudiation.

A PKI contains the following:

- Certificate Authority: CA is responsible for certificate issuing and revoking.
- Registration Authority: RA verifies the association of public keys with the legitimate holder.
- Central Directory: A secured location for storing and indexing keys.
- Certificate Management System: A system which comprises of generation, distribution, storage and verification of certificates. The format is defined in the X.509 Standard.

PKI uses asymmetric algorithm for digital certificate and digital signature scheme. Asymmetric algorithm (like RSA) generates a pair of keys. One of the keys is private and another public. Just as the name shows, public key is revealed in a certain way, while private key has concealed privacy.

Digital Signature with RSA is signing the message digest of content to produce the signature. As the message digest (hash of the content) is signed it consumes low bandwidth and space when transferring along with its content. Originator of message has a private key and a public key. With the private key, the message digest is signed and data is transmitted along with the signed content. The recipient fetches the public key of originator. He generates a message digest from the main content. Through the fetched public key the signature is decrypted to reveal the message digest. Both message digests are compared and if they match, signature is verified.

Public key cryptography is not an ideal scheme for security. It has an easy pit which can spoil entire purpose of cryptography. Say Bob sends a message to Peter. An imposter intercepts and sends his own public key to Peter. Peter considering it as Bob’s key, encrypts it using that and sends it to Bob, the imposter again intercepts and decrypt it with his own private key.

To prevent the above scenario, it is necessary to check the authenticity of the public key. Public key certification can resolve this problem. A digital certificate certifies the authenticity of public key and its holder. A trusted party like CA takes the information of the holder like
name, address, location etc. and binds it with public key. Before that CA verifies the proof of possession of public key claimed by its holder which can be through challenge-response or by proving the ownership of Private Key etc. CA then seals it with its private key. Anyone in the business with the public key must also have the public key of CA. X.509 is a standard certificate format that contains lot of information like version number, algorithm, Issuer name, validity period etc. [27]

**Revocation**

A certificate is valid for a certain period of time. However, certificates can be declared invalid for certain reasons like change in name, address or suspected to be compromised etc. In such situations, CA revokes the certificate. One of the certificate revocation methods is mentioned in X.509. CA signs and makes it available at public repository; this list is called CRL, certificate revocation list. CA signs the revoked certificate and this data structure is available in the CRL list along with time stamp. Revoked certificate has a serial number through which it is identified. An entity calling certificate also checks the serial number of the certificate against that CRL for validity verification. New CRL is kept issuing by the CA periodically.

### 4.1.1 Mobile PKI

Mobile PKI is often known as WPKI (Wireless PKI). The fundamental functions remained same; securing through integrity, authentication, non-repudiation and confidentiality by management of keys, cryptographic facilities and secure storage of signed data. Ensuring PKI standard in TCP/IP is unrealistic in case of WPKI, as WPKI deals with handheld devices whose processing power and memory is fairly weak in comparison.

Through GSM, two type of approach are there

1. SIM(Subscriber Identity Module)-Toolkit(STK) based PKI solution
2. WAP (Wireless Access Protocol) based security.

**SIM-Toolkit (STK) based PKI solution.**

STK based PKI solution is often a value added service, which is proprietary. It consists of several bodies that are in some sort of agreement with each other; they are the end user, mobile operator (MO), identity provider, CA, application provider [28].

Mobile operator plays an important and prime role in this scheme. Often it also acts as SIM provider. It can main the back end itself or by other parties.

Customer and corresponding SIM related information are registered in various sections. The identity of the client is saved in the database of MO and other parties also. CA uses the credentials to generate key pairs; the Private Key resides in the SIM card while Public Key in the back ends. The application in the SIM generates the key pair. A CSR (certificate signing request) is sent to the CA. CA signs it and the public key is stored in the back end. There are other ways also to generate the key pair based on the scenario the operator and their parties agree upon. For eg. CA can generate key pair and the private key and through the MO it can be issued to client including application. In mobile PKI authentication, the end user proves to
the identity verifier that he has the legitimate credentials [28]. A similar architecture of mobile PKI authentication is shown below:

![Figure 10: Mobile PKI Authentication Steps](image)

Request of end user goes to IDP via application provider. IDP verifies with back end server for the IMSI (unique id for SIM) and other credentials, checks with CA if certificate is still not revoked. If valid, IDP sends random challenge to the back end. Back end server sends a message (SMS but subscriber is not notified about that) with a request to sign the message. User is then asked to provide the PIN, after that the SIM application signs with the credentials and responses to IDP through the operator. This is how the authentication is done using STK based PKI.

### 4.1.2 WAP based PKI

WAP based security works on both GSM and GPRS technology. A WAP security comprises of WTLS (Wireless Transport Layer Security) for securing wireless part and SSL (Secured Socket Layer) for wired part. When WAP gateway catches the data through wireless medium, it then transfer to fixed internet, at that point there is protocol translation between WTLS and SSL. Figure 11 shows authentication through root CA’s certificate.

![Figure 11: Authentication through WPKI](image)
Data traffic travels between wired and wireless medium when WAP is used. Because of protocol translation end to end security is not there, rather WTLS and SSL takes responsibility separately.

The gateway server contains root certificate of CA which issues the content server’s certificate. Upon establishment of SSL connection, content server provides its digital certificate to WAP gateway. When content server communicates with wireless client, it authenticates itself by its certificate. The client therefore contains the root certificate of CA who has issued the certificate of gateway and that certificate is usually stored in WIM (Wireless Identity Module). Because of the limited processing and storing capability of wireless clients, a different certificate (WTLS certificate) is used in contrast to the certificates used for PKI in TCP/IP which provides strong security. An alternate approach is taken for checking the validation of certificates (e.g. CRL). WLTS certificates are issued for limited period each time [29].

4.2 SAFE System Overview

SAFE stands for Secure Application for Financial Environment. SAFE system is an integrated service to perform different financial services and some non-banking services. It supports person-person, bank-bank, and client-merchant transactions. The communication is circumvented with strong security features [30].

As described in [30] the main objectives of SAFE system are:

- Establishment and management of pre-prepaid accounts (PPAs) for individuals and business bodies.
- Using the pre-prepaid accounts for cash and account transfers, Point of Sale (PoS) payments.
- Issuing and managing biometric smart cards for merchant, clients, system admins and SAFE agents.
- Securing PPAs by using smart cards for authentication, authorization and payments.

Two uses of SAFE system is for Mobile Banking (m-Banking) and (m-Commerce).

**M-Banking:** This comprises of banking financial facilities for clients using mobile devices through GSM or wireless Internet.

Some of the financial services by m-Banking through SAFE systems are:

- Management of users’ account such as creation, queries related to transaction etc.
- Transfer of funds, digital cash among customers’ own account, others’ accounts, from other sources.

**M-Commerce:** Mobile commerce is a rapidly developing technology and it is possible that people can do almost all kind of financial transaction through m-Commerce.
Through the SAFE system, m-commerce mainly focuses on digital cash dispense and payment transactions.

As described in [30] mobile commerce can be used for the following services:

- Registering merchants and customers,
- Enrolment of merchants and customers for issuing SAFE smart card.
- Opening of merchant’s and customer’s PPAs associated with cards.
- Authenticating customers and verifying OTC payment.
- Depositing cash in customers' PPAs.

Two modes of transactions are possible via SAFE systems' m-Commerce.

a. **Over-the Counter**: Payment by customers using biometric chip and merchant uses compatible POS terminal.

b. **Over-the-air**: Payment is done by mobile phones, merchant and customers both uses mobile wallet in this case.

Two types of payment can be done:

- Digital Cash and micropayment
- Debit/Credit card payment.

Digital Cash is electronic value equivalent to cash. SAFE system can use this cash for micropayments. The POS of merchant should have compatible hardware and software preinstalled for successful micropayments [30].

1. The customer requests SAFE server for debit through CASH_REQUEST. Digital cash is stored in customer’s mobile wallet account after validation.
2. Customer pays at Merchant’s PoS terminal through his mobile phone.
3. PoS of merchant send a message to SAFE server (CASH_RECLAIM) which results in transfer of cash from merchant’s bank account to merchant’s account.

SAFE servers can process Credit or Debit Card Payment considering proximity protocol and compatible PoS is used by merchants. Merchants can request the SAFE server or Card Payment Gateway directly. Successful authorization provides successful transaction. Merchant then requests by sending CREDIT_REQUEST to SAFE server or payment gateway [30].
Chapter 5: Securing Magnetic Stripe Card-Data based on EMV Standard

The security of magnetic stripe based data is a great challenge considering that the data is ever static. In the proposed design, security is provided to the data, which is read by the Mobile Terminal from magnetic stripe card.

Following the EMV standard, following measures are taken to secure the related entities:

- Online card-data authentication of magnetic stripe.
- Offline card-data authentication of magnetic stripe.
  - Authenticating card-data by Offline SDA.
  - Authenticating card-data by Offline DDA.
- Card holder verification.
- Key management.
- Risk Management

Financial transaction demands concrete security. To provide better security and security related features, the concentration of the research was towards securing the Mobile Terminal to protect the magnetic card data and its holder. The reason of choosing a mobile as Terminal is because of its customizable and mobility features. Beside it is also user friendly. With the progress of time, the processing power and storage capability of mobile is increasing. Utilizing those features, more secured services, which consume memory, can be offered. But there are little things to do with fixed, traditional POS.

The differences between Mobile POS and Traditional POS are stated below:

**Table 9: Comparing Mobile POS and Traditional POS.**

<table>
<thead>
<tr>
<th>Mobile POS</th>
<th>Traditional POS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile POS systems are portable/mobile</td>
<td>Mostly stationary or limited wireless range.</td>
</tr>
<tr>
<td>Lower implementation cost</td>
<td>Implementation is costly.</td>
</tr>
<tr>
<td>Lower maintenance cost</td>
<td>Maintenance is costly.</td>
</tr>
<tr>
<td>Multiple POS when in rush hour</td>
<td>In most of the case, one POS due to expense.</td>
</tr>
<tr>
<td>Better security offered</td>
<td>Less security features offered.</td>
</tr>
<tr>
<td>Smooth update of POS software/application</td>
<td>Update procedure is complex</td>
</tr>
<tr>
<td>Security features can be upgraded/modified instantly upon authorization</td>
<td>Time consuming and restricted update service available.</td>
</tr>
<tr>
<td>Better customer service</td>
<td>Limited Customer Service.</td>
</tr>
</tbody>
</table>
5.1 Online Card-Data Authentication of Magnetic Stripe

In the traditional magnetic stripe card, the only secured component in the payment card used for authenticating and authorizing is the cryptogram, known as Card Validation Code (CVC). CVC contains the data of PAN and card-specific data and is encrypted using symmetric-key algorithm. As a part of securing the Online Card Authentication, the mobile Terminal does some additional task to produce a more secure cryptogram.

![Diagram of Online Card-Data Authentication of Magnetic Stripe]

**Figure 12:** Ensuring Authentication and Integrity of Merchant and Card

In the online authentication, symmetric Keys are used by the Issuer in two occasions. One pair of Key is shared between Issuer and Merchant and other pair between Issuer and magnetic card. After swiping, the mobile reads the card and captures the cryptogram (CVC). The customer then puts his PIN code and authorizes the transaction, the hash value of the transaction data and the CVC data is calculated. The key used is a symmetric key; one is kept to the Merchant and the other to the Issuer. The combined data and MAC is passed to Issuer. Issuer decrypts, compares the received hash value with its calculated value. Same MAC value ensures the integrity and authenticity of the cryptogram and authenticity of Merchant is also verified. Card verification is still left, which the Issuer completes by decrypting the card-cryptogram with its shared key (the shared key between Issuer and the magnetic stripe card). Thus the card is authenticated.
5.2 Offline Card-Data Authentication of Magnetic Stripe

Offline authentication is performed at the point of transaction, unlike online authentication where credentials are on the fly checked online. For securing the offline authentication, Public Key Cryptography based design is implemented. In the design, two offline authentication techniques are discussed: Static Data Authentication (SDA) and Dynamic Data Authentication (DDA). How these authentications are performed is discussed in the next section of this chapter. Both of the authentication methods have some common components/bodies taking part in securing the offline authentication, their role in authentication is described below:

Issuer

Issuer has the Issuer’s Private Key (SI). It signs the card data to produce Signed Card Data (SCD), in case of SDA which is SSAD (Signed Static Application Data).

Card Processor Company

Card Processor Company (EuroPay, Visa etc.) fetches the SCD/SSAD from Issuer. Each card thus has one corresponding SCD/SSAD stored with the Card Processor Company. The role of card Processor Company in offline authentication is to search and delivers the appropriate SSAD/SCD to Merchant when requested.

Certificate Authority

Certificate Authority (CA) signs the Issuer’s Public Key (PI). CA uses its Private Key (S_CA) to sign PI and produces Issuer PK Certificate, which is delivered to a Trusted Service Manager (TSM).

Certificate Authority

Certificate Authority (CA) signs the Issuer’s Public Key (PI). CA uses its Private Key (S_CA) to sign PI and produces Issuer PK Certificate, which is delivered to a Trusted Service Manager (TSM).

Trusted Service Manager

TSM is a trusted third party who is authorized to store and deliver specific credentials. For the offline authentication, TSM stores Issuer PK Certificate that it gets from CA, and Issuer Public Key of the CA (P_CA).

Merchant/Terminal

Merchant communicates with customer, TSM and Card Processor Company for the offline authentication purpose. Merchant uses a smart-phone as Point of Sales (POS). The card-reader attached with the smart phone reads the magnetic card and retrieves the data. The smart phone consists of secure micro SD card. This card is used as storage device as well as a smart card. This micro SD card has secure element and chip which allows it act like a smart card. The Merchant does not store the card data, signed card data, Issuer PK Certificate and CA Public key. The requests for those and processing are done instantly.

Customer

The customer bears the payment card (Debit/Credit Card). For payment, he gives swipes the card in the card reader attached to the merchant’s mobile terminal. The terminal reads the encoded data.
5.2.1 Authenticating Card-Data by Offline SDA

SDA is performed by Terminal. Through SDA, the legitimacy of the critical static data that the Merchant gets from Magnetic Card is confirmed. SDA also ensures that the merchant cannot alter the card-data without authorization.

![Diagram of SDA process]

Figure 13: Design of Static Data Authentication for Magnetic Stripe Card-Data

Figure 13 shows the component and process involved in Offline Static Data Authentication of the magnetic stripe card-data. Below it is described how Offline SDA is performed for Magnetic Stripe based transactions:

- Customer swipes the Magnetic Stripe Card in the POS (the card reader attached Mobile Terminal) and provides PIN code to authenticate.

- Merchant reads the card data, extracts the Card Number and Customer name along with other information. Merchant sends a message request (along with Card Number + Customer Name) for SSAD of that corresponding customer.

- Card Processor Company search through its database to find the match. Once found it sends the SSAD to Merchant. If not found, then it sends a response message SCD_NOT_FOUND.
• Transaction terminates if Merchant gets SCD_NOT_FOUND response. Else, Merchant sends a request message to TSM for the Issuer PK Certificate and CA Public Key.

• The TSM has the Issuer PK Certificate which it gets from Certificate Authority after CA signs the Issuer’s Public Key.

• Merchant verifies the Issuer Public Key by decrypting through CA Public Key. The Issuer Public Key is used to verify the SSAD; successful decryption verifies that Issuer signed this one.

![Diagram](CA_public_key_Issuer_PK_certificate_ISSued_public_key_authenticated.png)

Issuer Public Key authenticated

SSAD authenticated

Through the SDA authentication, it is verified that Merchant did not alter the card-data and the data is legitimate.

### 5.2.2 Authenticating Card-Data by Offline DDA

![Diagram](Design_of_Dynamic_Data_Authentication_for_Magnetic_Stripe_Card_Data.png)

**Figure 14:** Design of Dynamic Data Authentication for Magnetic Stripe Card-Data
Through Offline SDA, counterfeited or duplicate cards remain undetected. Dynamic Data Authentication (DDA) ensures the detection of counterfeited or duplicate cards. Figure 14 shows the design of performing this authentication. There is an additional pair of keys involved in DDA. The above figure shows parties involved in authenticating through offline DDA. The Secure Element of the Mobile Terminal has its own Private Key ($S_{IC}$), with which it can sign. It also has a Public Key ($P_{IC}$) which is used for encryption. $P_{IC}$ is certified by the Issuer; $S_{IC}$ and $P_{IC}$ both resides in the secure Micro SD Card, but the Private Key is not distributable, Public Key is distributable to authorized bodies.

Below it is described how Offline DDA is performed for Magnetic Stripe based transactions:

- Magnetic Stripe Card is swiped by the customer in the POS and he provides PIN code to authenticate.
- Mobile Terminal reads the card data, extracts the Card Number and Customer name along with other information. Merchant sends a message request (along with Card Number + Customer Name) for Secure Element (SE) PK Certificate to the Card Processor Company. The SE PK Certificate is the created by Issuer upon signing the Static Application Data (SAD) and Public Key of SE by Issuer’s Private Key.
- Card Processor Company searches for the appropriate card’s SE PK Certificate. Once found it is sent to the Merchant. If not found, then it sends a response message SE_DATA_NOT_FOUND.
- Transaction is terminated if Merchant gets SE_DATA_NOT_FOUND response. Else, Merchant sends a request message to TSM for the Issuer PK Certificate and CA Public Key.
- The TSM has the Issuer PK Certificate which it gets from Certificate Authority after CA signs the Issuer’s Public Key.
- Issuer Public Key is verified by the Merchant by decrypting through CA Public Key. The Public Key of Issuer is used to verify that Public Key of SE and Static Application Data (SAD) is Issuer certified. With the Public Key of Secure Element, it is verified that the dynamic data generated by Secure Element is digitally signed by it. This shows successful authentication of the data residing in Merchant’s Mobile Terminal, which was extracted from Magnetic Stripe Card.

This digital signature scheme prevents unauthorized alteration of data is every step. Beside as a result of using PKI, the whole system becomes highly scalable. Certificate exchange occurs among servers, clients and trusted parties only.

### 5.3 Cardholder Verification

The cardholder must be verified so that a fraud with duplicate or stolen card cannot perform transaction. This verification process verifies the legitimate card holder. If Merchant’s application is tampered and attempts replay attack to find out the PIN, random challenge used in the verification process stops such attack. The verification process goes as below:
The card holder swipes his magnetic stripe card in the reader attached to the Mobile Terminal. The Mobile shows the transaction details and asks for authorization. Card holder provides his PIN code.

Mobile Terminal sends a GET_CHALLENGE request to the Issuer.

The Issuer sends a random number challenge in response.

The customer provided PIN is encrypted by the shared Key of Merchant. As already discussed. Merchant and Issuer shares a secret key. The encrypted data along with the challenge is sent to Issuer.

Issuer authenticates the challenge, decrypts data with its shared Key to find out the PIN and verifies it.

Merchant acknowledged about successful PIN verification.

Customer’s PIN is accepted at Terminal.

The below figure summarizes the procedure.

---

**Figure 15:** Cardholder Verification with Enciphered PIN
5.4 Key Management

Key management is a crucial part of the security system, because due to mismanagement if secured keys are revealed then the whole security setup fails. Key management includes the generation of keys, storage of keys, key distribution of agreements and key verification. Protection mechanisms decide how to secure the cryptographic keys. For mobile devices, cryptographic key management is more crucial. For secure mobile transactions protection of cryptographic keys through layered hierarchy is necessary. Mobile devices can be lost/stolen and attacker can retrieve unprotected key to adversary can perform attack in several ways. Secure Elements (SE) have chips which can provide key management features.

Secure Elements can generate key pairs. Private keys cannot be accessed by anyone. If keys are stored in SE, only MIDlets who are authorized can access the keys for the run time only. SE is capable to perform what an ICC can do; so, same Key Management steps can be taken from Merchant’s mobile [22].

5.5 Risk Management

If a card is stolen or cloned, it is necessary that the perpetrator cannot figure out the PIN. For that reason if several wrong PIN are provided, the card should be blocked at the merchant’s POS and at the same time merchant’s mobile terminal will generate a message to Issuer. This will be a specific message format which will contain CVC1 information and pre-specified alert code for such incident, after getting that Issuer will block that card from processing transaction.

5.6 Analysis and Conclusions

In this research work, it is illustrated how the magnetic card based payment can be secured when used with Mobile POS. The purpose of the research was to provide a secure solution for magnetic stripe based payment. For this research we adopted Mobile Terminal as chosen POS because it is possible to implement varieties security features and services. Beside Mobile POS is portable and inexpensive. The security of Magnetic Card is beyond the scope of this research, one reason is the architectural limitation within static nature of the card. Instead focus is kept on securing the data that Mobile Terminal gets from the magnetic stripe card, verification of the card holder, Merchant and Issuer.

For achieving the desired service, we have used public key cryptography based design, the concept has been inherited from EMV specification.

The following security measures are taken:

- Online card-data authentication of magnetic stripe.
- Offline card-data authentication of magnetic stripe.
- Card holder verification.
- Key management.
- Risk Management
The research work proposed a security solution for the above areas and as a result the following security demands are met:

1. Confidentiality: achieved through cryptography through public key encryption.
2. Integrity: achieved by cryptography, calculating hash of data to check integrity.
3. Authentication: asymmetric algorithm ensured strong authentication.
6. Anonymity: cryptography ensured anonymity. Interceptor between merchant and Issuer can find only the cryptographic data, identity of customer remains encrypted.

## 5.7 Prototype

In order to demonstrate the proposed design, a prototype was implemented. The prototype is though a demo of the proposed idea, which has limited security features. It was developed as an additional service of SAFE System [30]. This is a payment add-on solution for m-Merchant, which is m-Payment. Authentication of card-holder and encryption of card-data is ensured in this service.

The designed mPayment is an complete card-payment solution, conducted through mobile. The mPay is the payment add-on for the merchant as described above. This is a payment part done through payments cards (EMV, Discovery etc.). The cardholder is the client or customer and the merchant holds the card-reader attached cell phone device with the payment application installed in it. Using this mobile wallet, the mPayment is done instantly and securely. As a payment gateway, SAFE Payment Server is used.

### Table 10: Description of Resources Used

<table>
<thead>
<tr>
<th>Resources</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC Operating System</td>
<td>9.04</td>
</tr>
<tr>
<td>Mobile Operating System</td>
<td>Android 2.2</td>
</tr>
<tr>
<td>Java</td>
<td>Version 1.7</td>
</tr>
<tr>
<td>IDE</td>
<td>Eclipse IDE for JAVA EE, version: 1.3.2</td>
</tr>
<tr>
<td>Android Development Tools</td>
<td>20.0.3.v</td>
</tr>
<tr>
<td>Card Reader</td>
<td>IDtech Unimag</td>
</tr>
<tr>
<td>Android SDK</td>
<td>API 8, Rev 3.</td>
</tr>
</tbody>
</table>
5.7.1 Implementation

Just like a traditional magnetic card based system, the customer swipes his card at the card-reader; the reader is attached with the merchant’s mobile phone (which is the POS in this case). The application asks to provide PIN. This PIN is provided by the customer during the registration phase, where he also provides other necessary information.

The customer selects the m-Pay options among other options for payment. A pop up menu will come up following the selection of m-Pay, with the payment options of Swipe Card, Bluetooth and NFC. For traditional swipe card based payments we will select Swipe Card, on which our security is imposed.

After selecting the Swipe Card option, the application detects the reader.

In the amount field, the merchant puts the amount to be paid. It is to be noted that the amount is “digital cash” here. After pressing the Swipe Card button, the authentication phase comes up. It asks the customer to put his PIN code.
On successful PIN entry, followed by pressing Swipe Card Button will transfer the fund to merchant’s account from customer’s account. The data that is passed from the merchant’s mobile terminal to payment gateway (SAFE Server) and is encrypted with shared key.

![Diagram of transaction flow]

**Figure 16:** Transaction from Customer’s Account to Merchant’s Account

### Communication with Bank Server

Customer’s credit/debit card information is pre registered with SAFE system. The customer registers his identity and also gets a PIN code for verification.

1. Customer swipes his debit/credit card to merchant’s PoS which is basically merchant’s Mobile Terminal attached with card reader. Merchant gets the card number.
2. Merchant sends the card number to SAFE portal for authorization.
3. Through the internal bank system, provided information is verified with customer’s account.
4. The digital cash is credited from Customer’s account.
5. Cash is deposited to Merchant’s account.
5.7.2 Summary

The initial work with the prototype started with interface designing. SDK was studied and a protocol was successfully designed which could read the magnetic stripe card's data through the reader. As a payment server, SAFE server is used for dispensing the digital cash from customer's account to merchant's account. Customer's information is extracted from the card, after he swipes his card in Merchant's Mobile Terminal; customers registered in SAFE systems are allowed to take part in the transaction. Extracted card number from the card is checked with database, if entry exists then transaction continues. Message and purchase amount is sent to SAFE Server, there money is transferred from customer's account to merchant’s account.

The next part was securing the prototype of the proposed design in this thesis. For that customer is verified by authenticating through PIN. In this way he also verifies the amount of money. The card data and transaction info is then encrypted and sent to SAFE Server. The SAFE Server and Merchant's mobile both shares a secret Key. Server decrypts with that Key and transaction continues like before.

5.7.3 Analysis and Conclusions

Financial applications are sensitive in terms of security. Threats and breach of security can make a good deal of damage. In order to provide a secured mobile application, the application was evaluated for security breach and unexpected behaviour and any bugs found were fixed. Though more secured solutions could have been provided, for example, RSA could have been used instead of symmetric key cryptography. But as the purpose was to provide a service which can be used by mass people, limitation of resources was also considered. Magnetic Stripe based transaction may not go on for couple of more decades, but many countries still using it. The proposed security solution in this thesis work ensures a mobile payment, which is vastly getting popular.
Chapter 6: Conclusions and Future Works

6.1 Conclusions

Smart phones are taking payment industry to a whole new arena. Processing power and memory of smart phones are enhancing with time. A couple of years before mPayment meant payment by Short Message Service, often which involved the operators and banks - services were proprietary. But now it is possible to perform the EMV or other payment card based transactions through merchants using mobile terminal. Traditional PoS is different in a number of ways compared to mobile PoS. Mobile PoSs are portable and also customizable. It is possible to execute update immediately in most of the cases, like upgrading the application or firmware of mobile.

Magnetic stripe is a fairly old technology. The motivation behind this research work was the huge popularity of magnetic stripe all over the World, especially in the developing countries where chip based technology is yet to implement. Cellular technologies are available in most of the countries. At the same time vulnerability and security breaches that cause payment fraudulence was something necessary to be dealt with. This research thus focused how we can blend the old and modern technology to provide a secured payment solution by using the swipe based payment technology.

In our research, we have used the security mechanism used by EMV industry for chip based payment solution. EMV standard is well known for its strong security features. It uses digital certificates and digital signatures through PKI for providing confidentiality, integrity, authentication and non-repudiation. In our research we did not considered WPKI for several reasons. First of all, a complete end-to-end security is not possible in either scenario, but through PKI strong authentication is possible. For WPKI, there are several changes necessary. Architecture for WPKI is based on low resource wireless devices. As a result, fewer credentials are used to generate certificate which might simplify the hard work for an attacker. There is no CRL, instead WPKI uses short lived certificate which requires accurate time awareness by client otherwise attacker can exploit security by expired (timed out) certificate. Elliptic curve cryptography is getting popular to be used in WPKI for key generation. ECC has six times less bits than RSS (164 against 1024) which will take less time for attacker through cryptanalysis. Hence our research prefers PKI usage for strong security.

We have conducted a demo of the proposed idea and successfully conducted a secured payment through magnetic swipe card. While magnetic stripe based cards can be replicated by perpetrator but an extra authentication as proposed and shown in the demo that can prevent unauthorized transaction.
6.2 Future Works

Chip and PIN (EMV) cards brought payment card fraud to a minimum level. With strong security features EMV cards will definitely beat the magnetic stripe cards out of the payment scenario in future. Despite this fact, it is also true that it will take time to fully migrate to chip enabled payment world. During this time there strategies are to be adapted to stop magnetic card based payment fraud.

One huge disadvantage of magnetic stripe card is the insecure transaction in while purchasing online (E-commerce). Static data is provided by the customer, for example the card number, card holder name, address etc. which can be skimmed easily by a fraud. A verification method can solve this problem. In our design, we used smart phones as Terminals. Customers can also use smart phone feature for card holder verification purpose. The smart phone will contain an authorized application (by Issuer or trusted third party). The application will produce a one-time password by combining card data and PIN code. The online merchant will verify the password with Issuer. This way card holder will be verified.

A big problem of static magnetic stripe is that has no processing capability. A new type of magnetic stripes based cards is there in the market which has powered magnetic stripes; a thin layer of Lithium ion batteries are embedded into the card body. These cards is also compatible with traditional readers. It can generate one time password, a feature which can be utilized to generate a dynamic. Thus the problem with static data can be resolved with this feature.
References


[30] Dr. Feng Zhang, March 2010. SECURE APPLICATIONS FOR FINANCIAL ENVIRONMENTS (SAFE) SYSTEM. KTH.

