

**PERFORMANCE AND SECURITY ISSUES IN E-PAYMENT  
SYSTEMS:  
PAY ON-LINE CASE**

**ORHAN KARAHASAN**

**IŞIK UNIVERSITY  
2006**

**PERFORMANCE AND SECURITY ISSUES IN E-PAYMENT SYSTEMS:  
PAY ON-LINE CASE**

**A Thesis  
Presented to the Institute of Science and Engineering  
of  
Işık University  
In Partial Fulfillment of the Requirements for the Degree of  
Master of Science  
in  
The Department of Computer Engineering**

**by  
Orhan Karahasan**

**June 2006**

Approval of the Institute of Science and Engineering

\_\_\_\_\_  
Prof. Dr. Hüsnü Erbay  
Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science.

\_\_\_\_\_  
Prof. Dr. Selahattin Kuru  
Head of Department

This is to certify that we have read this thesis and that in our opinion it is fully adequate, in scope and quality, as a thesis for the degree of Master of Science.

\_\_\_\_\_  
Prof. Dr. Selahattin Kuru  
Supervisor

Examining Committee Members

|       |       |
|-------|-------|
| ..... | _____ |
| ..... | _____ |
| ..... | _____ |
| ..... | _____ |
| ..... | _____ |

## **ABSTRACT**

### **PERFORMANCE AND SECURITY ISSUES IN E-PAYMENT SYSTEMS: PAY ON-LINE CASE**

Karahasan, Orhan

In this thesis, we report an experience on Performance and Security issues in E-Payment systems. We develop an E-Payment system which covers all introduced performance and security measures written in this thesis. We also compare different types of means that can be used in E-Payment systems. We mentioned different types of network architectures, and their benefits and drawbacks for E-Payment systems. An example e-payment system called Pay ON-LINE is developed with the proposed security and performance architectures. This system is in use in Şile campus of Isik University.

Keywords: Performans, Security, E-Payment Systems

## ÖZET

### PERFORMANCE AND SECURITY ISSUES IN E-PAYMENT SYSTEMS: PAY ON-LINE CASE

Karahasan, Orhan

Bu çalışmada Elektronik Ödeme Sistemleri için kullanılabilir çeşitli araçlardan bahsedilmiştir. Bunların karşılaştırması yapılmış ve çeşitli isterler için uygulanması gereken araçlar listelenmiştir. Ödeme sistemlerinde en önemli konulardan biri olan güvenlik konusu çeşitli yönleri ile ele alınmıştır. Performans konusunda bazı yeni teknikler tanımlanmıştır. Bu çalışmada ortaya atılan yeni performans ve güvenlik ölçütlerinin uygulaması anlatılmıştır. Verilen güvenlik ve performans mimarilerinin bir uygulaması olan Pay ON-LINE elektronik ödeme sistemi geliştirilmiştir. Bu uygulama Işık Üniversitesi Şile Kampus'ünde elektronik ödeme sistemi olarak kullanılmaktadır.

Anahtar Kelimeler: Elektronik Ödeme Sistemleri, Performans Artımı, Güvenlik

to my family

## **ACKNOWLEDGEMENTS**

I would like to express my deepest gratitude to all those who contributed directly or indirectly to bringing this publication to this final format, because I would never have been able, by myself, to achieve this.

My most sincere gratitude and appreciation are dedicated to Prof. Dr. Selahattin Kuru, my supervisor, for his inspirational guidance, invaluable suggestions and endless motivation. Many thanks to Mustafa Yıldız, Onur İhsan Arsun, and Gürol Erdogan, my colleagues, for their personal and professional support and for being closest friends.

Finally, I wish to record my special thanks to my parents, for their endless love and confidence.

## TABLE OF CONTENTS

|  |      |
|--|------|
| ABSTRACT .....   | ii   |
| ÖZET .....   | iii  |
| ACKNOWLEDGEMENTS.....  | v    |
| TABLE OF CONTENTS .....                                      | vi   |
| LIST OF FIGURES.....   | viii |
| LIST OF TABLES .....   | x    |
| 1. INTRODUCTION .....  | 1    |
| 2. E-PAYMENT CARD TECHNOLOGIES AND SYSTEM ARCHITECTURES..... | 3    |
| 2.1. E-Payment Technologies.....                             | 3    |
| 2.1.1. Barcode .....   | 3    |
| 2.1.2. Magnetic Cards.....                                   | 7    |
| 2.1.3. Proximity Cards.....                                  | 10   |
| 2.1.4. Vending Tags.....                                     | 10   |
| 2.1.5. Smart Cards.....                                      | 12   |
| 2.1.6. Combi Cards.....                                      | 22   |
| 2.2.E-Payment Architectures.....                             | 24   |
| 2.2.1. Online.....   | 24   |
| 2.2.2. Semi On-Line.....                                     | 24   |
| 2.2.3. Offline.....  | 25   |
| 3. SECURITY IN E-PAYMENT SYSTEMS.....                        | 27   |
| 3.1.Physical Security.....                                   | 32   |
| 3.1.1. Terminal Monitoring Software.....                     | 32   |
| 3.1.2. Network Architecture.....                             | 34   |
| 3.2.Data Security.....                                       | 37   |
| 3.2.1. Cryptography.....                                     | 37   |
| 3.2.2. Epayment Mean Security.....                           | 43   |
| 4. PERFORMANCE IN E-PAYMENT TECHNOLOGIES.....                | 44   |
| 4.1.In Polling Based Systems.....                            | 45   |
| 4.2.In Hand Shaking Based Systems.....                       | 45   |
| 4.2.1. Data Loss.....  | 47   |



|   |    |
|---|----|
| 5. APPLICATION OF SECURITY AND PERFORMANCE ARCHITECTURES..... | 48 |
| 5.1.PAY ON-LINE:An Example Application .....                  | 48 |
| 5.2.SECURITY ARCHITECTURE of Pay-Online.....                  | 48 |
| 5.3.PERFORMANCE ARCHITECTURE.....                             | 51 |
| 5.3.1. Performance statistics.....                            | 52 |
| 6. CONCLUSION AND RECOMMENDATIONS .....                       | 53 |
| REFERENCES .....  | 54 |
| APPENDICES.....   | 57 |
| A.1. Descriptions of Database Tables .....                    | 57 |
| A.2. Definitions of Database Tables .....                     | 58 |
| A.3. Database Diagram .....                                   | 61 |
| A.4. Pay-ONLINE Terminals.....                                | 62 |
| A.5. Pay-ONLINE Modules .....                                 | 84 |
| A.6. Pay-ONLINE Users.....                                    | 88 |

## LIST OF FIGURES

|              |   |    |
|--------------|---|----|
| Figure 2.1   | Physical Dimensions of magnetic Cards .....                       | 8  |
| Figure 2.2   | ISO 7811 Standard Data Structure.....                             | 9  |
| Figure 2.3   | Proximity Card Example .....                                      | 10 |
| Figure 2.4   | Vending Tag Example.....  | 11 |
| Figure 2.5   | Contact Smart Card.....   | 16 |
| Figure 2.6   | Contactless Smart Card.....                                       | 17 |
| Figure 2.7   | CombiCard.....  | 23 |
| Figure 2.8   | Online Working Systems.....                                       | 25 |
| Figure 2.9   | Semi Online Working Systems.....                                  | 26 |
| Figure 3.1   | Goals of Security .....   | 28 |
| Figure 3.2   | Security Attacks.....   | 31 |
| Figure 3.3   | Flowchart diagram for Terminal Status Function.....               | 33 |
| Figure 3.4   | Open Network Architecture.....                                    | 35 |
| Figure 3.5   | Closed Network Architecture.....                                  | 36 |
| Figure 3.6   | Modified Open Network Architecture.....                           | 36 |
| Figure 3.7   | Private Key Encryption.....                                       | 40 |
| Figure 3.8   | Automatic Key distribution for Connection Oriented Protocol..     | 41 |
| Figure 3.9   | Asymmetric Encryption System.....                                 | 43 |
| Figure 4.1   | Network Architecture for E-Payment System.....                    | 44 |
| Figure 4.2   | Handshaking Process Diagram.....                                  | 47 |
| Figure 4.3   | Pseudo code for transaction transfer from terminal to server..... | 48 |
| Figure 5.1   | Process diagram for key exchange and data transfer.....           | 49 |
| Figure 5.2   | Terminal Monitoring Software.....                                 | 50 |
| Figure 5.3   | Network Arcitecture of Pay ON-LINE.....                           | 51 |
| Figure A.3.1 | Database Diagram .....  | 61 |
| Figure A.4.1 | Dining Hall Operation Interface .....                             | 63 |
| Figure A.4.2 | Dining Hall Shift Report .....                                    | 63 |
| Figure A.4.3 | Market Operation Interface .....                                  | 64 |
| Figure A.4.4 | Market Shift Report .....   | 65 |
| Figure A.4.5 | Manual Loading Center Operation Interface .....                   | 66 |

|               |  |    |
|---------------|--|----|
| Figure A.4.6  | Manual Loading Center Credit Card Interface.....       | 66 |
| Figure A.4.7  | Manual Loading Center PIN Interface .....              | 67 |
| FigureA.4.8   | Manual Loading Center Cancel Operation Interface ..... | 68 |
| Figure A.4.9  | Manual Loading Center Shift Report .....               | 68 |
| Figure A.4.10 | Automatic Loading Center .....                         | 69 |
| Figure A.4.11 | Leisure Center Operation Interface .....               | 70 |
| Figure A.4.12 | Leisure Center Shift Change Interface .....            | 70 |
| Figure A.4.13 | Leisure Center Shift Report .....                      | 71 |
| Figure A.4.14 | PDA Operation Interface .....                          | 71 |
| Figure A.4.15 | Hot Vending Machine .....                              | 72 |
| Figure A.4.16 | Cold Vending Machine .....                             | 72 |
| Figure A.4.17 | Combi Vending Machine .....                            | 73 |
| Figure A.4.18 | Pay ON-LINE Web Interface .....                        | 74 |
| Figure A.4.19 | Pay ON-LINE Accounting Officer Functions .....         | 74 |
| Figure A.4.20 | Pay ON-LINE Card Transaction Report Interface .....    | 75 |
| Figure A.4.21 | Pay ON-LINE Accounting Officer Functions .....         | 76 |
| Figure A.4.22 | Pay ON-LINE Subcontractor Report Interface .....       | 76 |
| Figure A.4.23 | Pay ON-LINE Meal Transaction Report .....              | 77 |
| Figure A.4.24 | Pay ON-LINE Loading Center Report .....                | 77 |
| Figure A.4.25 | Pay ON-LINE Card Owner Transaction Report .....        | 78 |
| Figure A.4.26 | Pay ON-LINE Automatic Loading Center Report .....      | 79 |
| Figure A.4.27 | Pay ON-LINE General Report Interface .....             | 79 |
| Figure A.4.28 | Pay ON-LINE total spending/loading report .....        | 80 |
| Figure A.4.29 | Pay ON-LINE Feedback Interface .....                   | 80 |
| Figure A.4.30 | Pay ON-LINE Card Owner Functions .....                 | 81 |
| Figure A.4.31 | Pay ON-LINE Card Owner Report Interface .....          | 81 |
| Figure A.4.32 | Pay ON-LINE Feedback Interface .....                   | 82 |
| Figure A.4.33 | Pay ON-LINE Subcontractor Report Interface .....       | 82 |
| Figure A.4.34 | Pay ON-LINE Feedback Interface .....                   | 83 |
| Figure A.5.1  | Card Initialization Interface .....                    | 85 |
| Figure A.5.2  | Terminal Monitoring Software Interface .....           | 86 |
| Figure A.5.3  | Data Transfer Module Interface .....                   | 86 |

## LIST OF TABLES

|           |  |    |
|-----------|--|----|
| Table 3.1 | Some Information on Security Objectives..... | 37 |
| Table 5.1 | Memory CPU usage during data transfer.....   | 52 |

# CHAPTER 1

## INTRODUCTION

E-Payment means that the payment procedure is handled in digital environment such as credit cards, campus card systems, or etc. Nowadays, most of the payment transactions are done electronically. In 2005 e-payment transactions increase 138% according to the eCompany[1].

To build an e-payment system, there are different types of network architectures; e-payment means (such as vending tags, smart cards, etc) can be used. Typically there are two parts of the payment systems. One is the terminal on which the payment transactions can be done, and one is the server on which the final data is collected on from the terminals.

The electronic payment system eliminates the usage of conventional money. The system may use proximity cards, barcode technology or smart cards for all transactions. Advanced reporting tools make transaction control convenient for upper management.

The electronic payment system can be integrated to vending machines, washing machines, copying machines and so forth.

The POS terminals can be handhelds, computers, or specially designed POS machines.

First of all, there are different card technologies that can be used in payment transactions. First, those technologies will be mentioned. There are 6 different card technologies are most commonly used in payment systems, which can be called as e-payment technologies. Those technologies are namely; barcode technology, magnetic card technology (which were common in credit cards), proximity cards, vending tags, smart cards and combi cards that combines more than one technology.

Secondly, different network architectures defined between the components of the payment systems. Those network architectures are mentioned in the second part of the second chapter. Those architectures will be compared and pros and cons of those architectures will be clearly defined. Network architecture is very important based on non-functional requirements such as security, reliability, availability, performance, etc.

Thirdly, security of e-payment systems will be discussed under several topics. Those topics are under physical security and data security. I try to find the best solution for the security of e-payment system. Data security is very important for e-payment systems, because any change on the system will cause numerous problems depending on the change of debit or credit values of the payment means.

After the security chapter, performance of e-payment systems will be discussed. For those type of transaction based systems, performance becomes one of the first non-functional requirements of the system. For performance, there will be some techniques introduced for data transfer between the server and the terminals. Also for the performance increase in data retrieval for reporting services will be discussed.

Finally, the platform is built on the e-university infrastructure of Işık University and an example e-payment application is developed which is working at the Şile Campus of Işık University, namely Pay ON-LINE that is the application of proposed security and performance architectures. Pay ON-LINE is a member of e-university tools family which includes Campus ON-LINE [2], the course registration and student information system; Course ON-LINE [3], course homepages management system and CAMPUS ON-SMS [4], information distribution system over SMS. All of these tools are fully integrated with each other and share a common database.

## **CHAPTER 2**

### **E-PAYMENT CARD TECHNOLOGIES AND SYSTEM ARCHITECTURES**

In e-payment systems there are many card technologies that can be used. In this chapter, those technologies will be listed. At the end the comparison of those technologies will be made. In the second part of this chapter, different architectures that can be used for e-payment technologies will be introduced and their comparison will be made.

#### **2.1. E-Payment Card Technologies**

The card technologies that can be used for e-payment systems are barcode, magnetic card, proximity card, vending tags and smart cards. The combination of those card technologies can also be used as a card technology for an e-payment system.

##### **2.1.1.Barcode**

Bar codes are machine-readable symbols made of patterns of black and white bars and stripes, or in some cases checkerboard-like grids [5]. There are different styles of bar codes called symbologies. Code 39, UPC, and Code 128 are examples of different symbologies.

Bits of information are encoded within bar codes. The data is read by bar code scanners and is often used in conjunction with databases. Bar codes don't require human-input, can be read by automated machines, and is virtually error-free [6].

Bar codes are used on anything in the retail channel destined to be scanned at the cash register. They're also used on everything from shipping forms, labels, ID cards, direct mail pieces, and invoices.

Scanners look at the pattern of light and dark bars and decode a bar code, returning the string contained in them. Often this string is a look-up into a database. That's how the grocery store cash register knows that you just bought a box of cereal for \$2.59. The UPC bar code contains a number that matches a record in the store's database. Neither the item's name nor its price is in the bar code. It's just a record number that references a database.

Using a font to create a bar code is quick and easy. You can use a font from within your favorite Microsoft Windows or Macintosh applications including databases, spreadsheets, word processors, and desktop publishing applications. Unlike graphic images, there is no storage requirement because the bar codes are made dynamically by formatting the correct string in a bar code font.

Bar code systems can use several symbologies. A symbology is equivalent to a language. Each symbology has strengths and weaknesses. Many symbologies are around for historical or political reasons, while others have definite technical advantages.

In many systems, you must conform to a company-specified symbology. If this is the case, then you don't have much choice unless you can give the company a good reason to change. In other systems, you are given the choice to use any symbology you wish. Choose your symbology carefully. The symbologies and their explanations are as given below.

### ***Code 128***

This symbology is a very compact bar code for all alphanumeric applications. The full (128-character) ASCII character set can be encoded in this symbology without the double characters found in extended Code 39. If the bar code has four or more consecutive numbers (0-9), the numbers are encoded in double-density mode (where two characters are encoded into one character position). Code 128 also has five special, nondata function characters. These are generally used to set reader parameters or return parameters. Code 128 actually has three different character-code



subsets. It has two forms of error checking, making it a very stable bar code. Checksums are not required. If you have your choice, Code 128 is generally the best all-around choice you can use.

### ***Code 39***

Code 39 (or Code 3 of 9) is the most common bar code in use for custom applications. It is popular because it can support both text and numbers (A<Z, 0<9, +,-, ., and ), it can be read by almost any bar code reader in its default configuration, and it is one of the oldest of the modern bar codes. Code 39 is a variable-width bar code, and it can support any number of characters that the reader can scan. Code 39 is specified in many military and government specifications. Code 39 bar codes are self-checking and are not prone to substitution errors. They generally do not require checksums.

### ***Interleaved 2 of 5***

Also known as I2of5, this is a numeric-only bar code that prints out a little larger than the UPC-A bar code when 10 digits are encoded. This symbology has the flexibility to encode any even number of digits. If you have an odd number, a leading zero is added. This bar code is an excellent candidate for numeric-only applications, and it is the best symbology to use for fixed-mount readers. Because Interleaved 2 of 5 is prone to substitution errors, you should always use a checksum.

### ***UPC (Universal Product Code)***

UPC is the standard bar code for items for sale to the public. It is the code seen on items at the local supermarket. UPC-A is a fixed-length, numeric-only bar code. It contains 1 digit for a system number, 5 digits for the manufacturer number, 5 digits for the product number, and one checksum digit. The position and value of the digits is standardized by a grocery industry committee. UPC-A and UPC-E also allow two- or five-digit supplemental numbers. UPC-A and UPC-E codes have an automatic checksum. UPC-E is ideal for small packages, because it is the smallest bar code available. This symbology contains the same information as UPC-A, except that at least four zeros are suppressed. Only tags with the system character of 0 can be

encoded with this symbology. UPC-A and UPC-E codes have an automatic checksum. Interleaved 2 of 5 is almost as dense and does not have the format considerations.

### ***Extended Code 39***

Extended Code 39 is a derivative of Code 39. This symbology uses combinations of two standard Code 39 characters for every character in the ASCII character set (0-127). This symbology allows lowercase letters and control characters, at the expense of size. This makes the code very big if you have very many lowercase or special characters. Most bar code readers in their default configuration will not read Extended Code 39. If you want to use this symbology, you will probably need to configure the reader. If you need to read both uppercase and lowercase, you should use Code 128.

### ***Code 93 and Extended Code 93***

Code 93 and Extended Code 93 are compressed versions of Code 39 and Extended Code 39. This symbology supports the same characters as Code 39, but in a smaller character width. This is a more difficult symbology to read, and many readers do not support it. Both Code 93 and Extended Code 93 have automatic checksums.

### ***UCC 128***

This bar code is a 19-digit, fixed-length bar code that uses Code 128 C to generate the bar code. This bar code is specifically used on shipping containers by those who ship items with UPC codes. UCC 128 has automatic checksums.

### ***Codabar***

Codabar bar codes can include numeric characters, six punctuation characters (-\$/./+), and spaces. There are also four special start/stop characters, which are A, B, C, and D. Codabar is useful for encoding dollar figures and mathematical figures. These bar codes are slightly larger than Interleaved 2 of 5 bar codes. Codabar requires start and stop characters. The Codabar symbology is self-checking, but you can use a mod 16 or mod 10 checksum.

## ***EAN/JAN***

The EAN/JAN-13 code is used for overseas applications where a country code is required. The UPC-A symbology is actually a subset of the EAN/JAN-13 symbology. This bar code is composed of 2 numbers for the country code, 10 numbers for the data characters, and a checksum. The checksum is generated automatically. The EAN/JAN-8 code is also used for overseas applications where a country code is required. This is similar to the EAN/JAN-13 except that only 5 numbers are used.

## ***MSI***

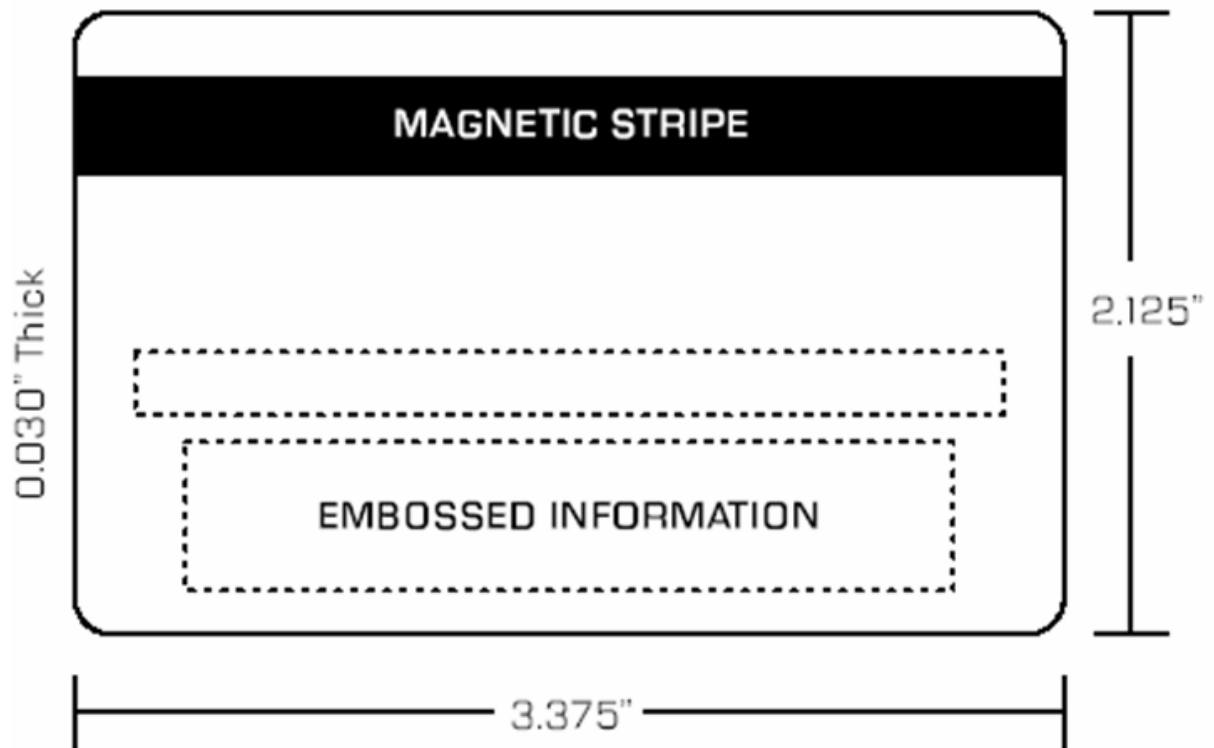
The MSI bar code is used most often in the grocery industry for shelf labels. This is a numeric-only code that stands up well to wear and tear. This code is not self checking, and so a checksum is highly recommended. It supports three types of checksums.

## ***2D (Two-Dimensional) Bar Code Symbologies***

A 2D bar code symbology allows vast amounts of data on a single bar code by storing data in 2 dimensions. A common demonstration of the technology is a single bar code no larger than a standard UPC bar code that contains the entire Gettysburg Address. Some common 2D bar code symbologies include PDF 417, DataMatrix Code, and MaxiCode.

### **2.1.2. Magnetic Cards**

Magnetic cards are another card technology that can be used for e-payment systems. Actually the most widely used card technology is magnetic stripe cards. A half-inch wide strip magnetic tape is bonded to the card substrate. The individual magnetic particles are aligned along the stripe, but when encoded, the individual particles may be magnetized either from left to right or from right to left, so there is no overall polarization. Blank white cards with a magnetic stripe can be freely purchased from card manufacturers and dealers. Physical dimensions of a magnetic card is given in Figure 2.1.



**Figure 2.1. Physical Dimensions of Magnetic Cards**

### *Encoding and decoding*

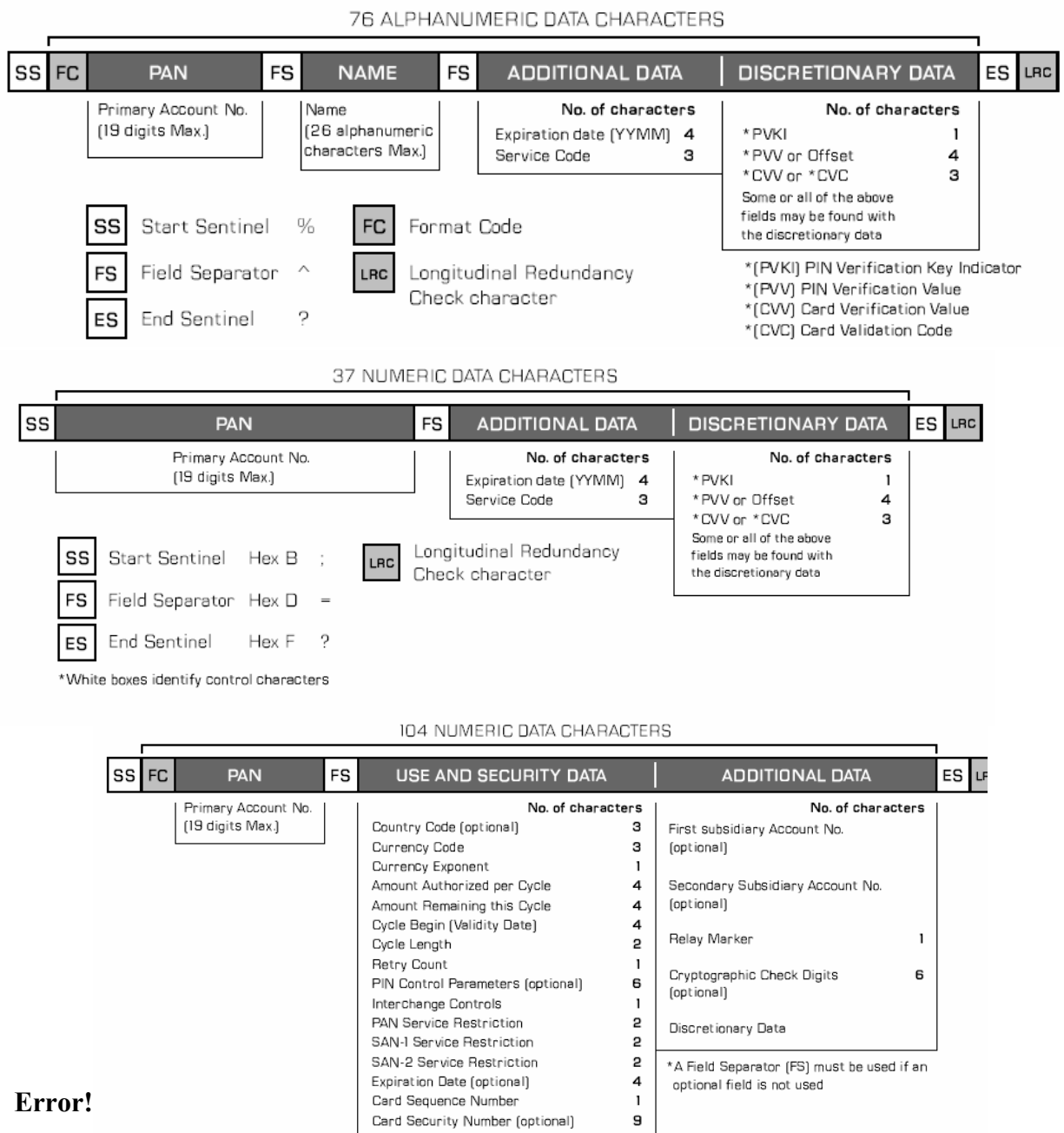
To encode the stripe, a magnetic field is applied using coil-wound magnetic head; this results in all the particles being polarized the same way. When the encoding current is reversed, the polarization also reverses.

The stripe is read by passing the card in the front of a reading head, each polarization reversal results in a pulse of current in the coil, positive or negative depending on the direction of the reversal.

These pulses must then be decoded into 0s, and 1s: Several different encoding schemes are possible, but the most common is known as F/2F. In this scheme, a 0 and a 1 are the same length. A 0 is a single domain with no flux reversal, while a 1 has a flux reversal in the middle.

### *Standards*

There are two standards defining the magnetic stripe cards. Those are namely; SO 7811 and ISO 7810. ISO 7811 defines the coding schemes for the magnetic stripe cards as well as the track information on the cards. According to this standard; there are three different tracks. On the first track; you can store 79 alphanumeric characters. On the second one; you can only store 40 numbers. On the last track; there are 107 numbers stored. The track information of a magnetic card is given in Figure 2.2.



**Error!**

**Figure 2.2. ISO 7811 Standard Data Structure**

### 2.1.3. Proximity Cards

The typical proximity card consists of a microchip and antenna embedded in a plastic card [9]. When the card is placed within the radio field of the reader, the energy broadcasted from the reader energizes the microchip on the card and begins a transaction between the card and reader. When the reader recognizes the card, the card is queried for the identification number. A proximity card can be passive or active. An active card has a battery to power the microchip and is usually thicker than the standard ISO plastic card. A passive card depends solely on the radio field of the reader for power giving it less range but longer useful life. Proximity readers have been steadily gaining in popularity because of the ease of use, lack of wear, and high tech image. The cards are very difficult to duplicate because of the need for the microchip, knowledge of radio technology, and the software needed to implement the protocol. The minor problems associated with this technology are occasional problems with RF interference and the fact that it may be easier to follow someone with valid access through a door because the read range may make it more difficult for a guard to verify that a person has or has not presented a card. Sample proximity card is given in Figure 2.3.



Figure 2.3. Proximity Card Example

### 2.1.4. Vending Tags

Vending tags uses the same technology like used in the proximity cards. The labels used for the identification purpose is placed just inside a different product rather than cards. Those tags are working with RFID technology. They can only be read. In other words, they are read-only [10]. Sample vending tag is given in Figure 2.4.



Error!

**Figure 2.4. Vending Tag Example**

There are two different types of labels that are used in vending tags.

### ***Inductively Coupled RFID Tags***

This type of RFID tag has been used for years to track everything from cows and railroad cars to airline baggage and highway tolls. There are three parts to a typical inductively coupled RFID tag:

- **Silicon microprocessor** - These chips vary in size depending on their purpose
- **Metal coil** - Made of copper or aluminum wire that is wound into a circular pattern on the transponder, this coil acts as the tag's antenna. The tag transmits signals to the reader, with read distance determined by the size of the coil antenna. These coil antennas can operate at 13.56 MHz [11].
- **Encapsulating material** - glass or polymer material that wraps around the chip and coil

Inductive RFID tags are powered by the magnetic field generated by the reader. The tag's antenna picks up the magnetic energy, and the tag communicates with the reader. The tag then modulates the magnetic field in order to retrieve and transmit data back to the reader. Data is transmitted back to the reader, which directs it to the host computer.

### ***Capacitively Coupled RFID Tags***

Capacitively coupled RFID tags have been created in an attempt to lower the cost of radio-tag systems. These tags do away with the metal coil and use a small amount of silicon to perform that same function as a inductively coupled tag. A capacitively coupled tag also has three parts:

- **Silicon microprocessor** - RFID tags use a silicon chip that is only 3 mm<sup>2</sup>. These tags can store 96 bits of information, which would allow for trillions of unique numbers that can be assigned to vending tags.
- **Conductive carbon ink** - This special ink acts as the tag's antenna. It is applied to the paper substrate through conventional printing means.
- **Paper** - The silicon chip is attached to printed carbon-ink electrodes on the back of a paper label, creating a low-cost, disposable tag that can be integrated on conventional product labels.

By using conductive ink instead of metal coils, the price of capacitively coupled tags are as low as 50 cents. These tags are also more flexible than the inductively coupled tag. Capacitively coupled tags, like the ones made by Motorola, can be bent, torn or crumpled, and can still relay data to the tag reader. In contrast to the magnetic energy that powers the inductively coupled tag, capacitively coupled tags are powered by electric fields generated by the reader.

### **2.1.5. Smart Cards**

A smart card is a device that has both processing power and memory, and is capable of being packaged in the format defined by the International Standards Organization (ISO). The standard that defines the Integrated Circuit cards is ISO 7816 [12]. To be more precise, the ISO uses the term, Integrated Circuit Card (ICC) to



encompass all those devices where an integrated circuit is contained within an ISO ID1 identification card piece of plastic.

It is similar in appearance to a credit card, but has a microcomputer chip embedded into it that can produce as much power as some personal computers; some consider it to be the next generation of portable computer. The microcomputer is able to store and manipulate data, and solve mathematical problems. The microchip has 60 times more memory than a conventional magnetic strip card.

Due to its added intelligence of a microprocessor, size and computing ability, it can afford greater security and hence has many applications in various area. Currently, smart cards are used for payment of telephone calls, payment of parking and tolls, storage of identification and medical records, and access to satellite television, among other applications.

### ***Elements of a typical Smart Card***

Smart cards have the same three fundamental elements as all other computers: processing power, data storage and a means to input and output data. Processing power is supplied by a microprocessor chip (e.g. Intel 8051 and Motorola 6805), and data storage is supplied by a memory chip (EEPROM, FLASH, ROM, RAM). In some instances these elements can be combined in one chip. The means in which data is transferred varies from card to card. In order to operate, each card must have a power source, whether in a card reader or on the card itself [13].

- ***Microprocessor***

The microprocessor is the intelligent element of the smart card which manipulates and interprets data. The software utilized for manipulation and interpretation of the data is either embedded in memory during the manufacture of the card or input under the control of the microprocessor . Microprocessors in smart cards can be up to 16 bits with a 10MHz processor (Clark and Hoffman 1994).

- ***Memory***

The memory in a smart card can either be non-volatile, retaining data when power is switched off, or volatile, losing data when power is switched off. If the memory is volatile, the smart card would then require a battery to power itself. Memory can also allow data to be written to it and read from it, or only allow data to be read from it (read-only memory). In most cases smart card applications will require non-volatile memory to retain information such as the identity of the cardholder and the application software, and read/write memory to update stored information, such as a balance after a transaction is made .

Memory in smart cards can be categorized into three types: ROM, RAM and programmable read-only memory (PROM). ROM is non-volatile, and the contents are embedded in the chip during the manufacturing stage; once embedded, the contents cannot be altered . Currently, chips with up to 32Kb of ROM are available. RAM is volatile, and is used as a temporary storage space. Data can be written to it, altered, read and deleted from it . Currently, chips are available with more than 64Kb of RAM . There are two types of PROM: electrically programmable read-only memory (EPROM) and electrically erasable programmable read-only memory (EEPROM). EPROM cannot be reprogrammed. EEPROM can be reprogrammed, however its structure is more complex and susceptible to damage which makes it more expensive . Currently, chips with up to 8Kb of EEPROM are available.

Memory can be structured to provide different levels of security zones. The open zone holds non-confidential data, such as identity of the cardholder, but cannot be altered by an unauthorized person. The working zone holds confidential data that requires certain information to be given before access is allowed. For instance, a personal identification number (PIN) would be required before accessing the data for a purchase transaction and available credit. The secret zone holds completely confidential data, such as the PIN. The microprocessor can access this data to compare the PIN to the number input by the cardholder, which ensures the data never leaves the card .

- ***Input / Output***

There are several different ways to input and output data to and from the smart card. Contact cards usually contain a metallic contact on the surface which, when

inserted in a slot in the read/write unit (e.g. Smart Card Reader), links with a connector in the unit. Contactless cards use a contactless method of transmission and reception of data, which only require the card to be placed near or on the surface of the read/write unit . Super Smart Cards have an integrated keyboard and display unit, therefore not requiring a read/write unit. They may have contacts embedded in the surface of the card in order to transfer data to other electronic devices .

- ***Power Source***

Generally, there are three methods used to power smart cards:

- ***From an external power source that feeds a current through contacts on the card***

In this method, power is sent through two of the contacts when the card is inserted in the read/write unit. The card will then reset itself, and execute its program [14].

- ***By transmitting power***

In the second method, a type of contactless operation such as inductive coupling will transmit both power and data through the air or a non-metallic surface to the smart card, from the read/write unit [15].

- ***By a battery embedded in the card***

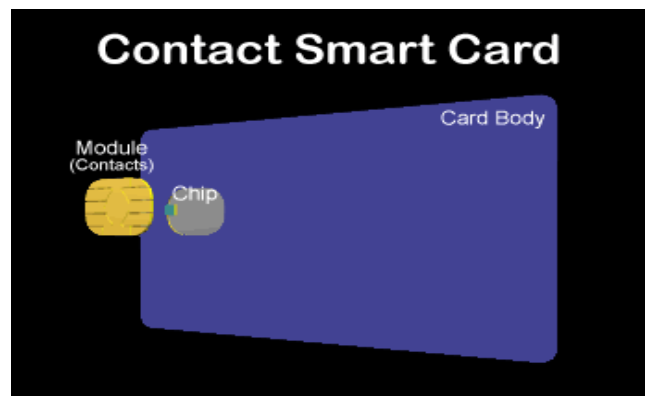
In the third method, a battery is incorporated in the card. This method is not popular due to the difficulty of meeting the ISO standards for dimensions, additional costs incurred from incorporating the battery in the card and problems associated with flexing a card containing a battery .

### ***Types of Smart Cards***

Depending on how the smart card is accessed, smart card can be classified into 4 main type:

- ***Contact Smart Cards***

These cards have a microelectronics embedded in the cards, with connections to metallic contact pads on the surface of the card (usually a small gold chip about 1/2" in diameter). The contacts link with the read/write unit (Smart Card Reader) to enable the microcomputer to communicate and provide power to the microelectronics. There are a total of eight contacts: two are reserved for future allocation, two for supply voltage and ground, one for reset, one for the clock signal to provide timing for the microprocessor, and the remaining for input and output of data and power. The standard position for the contact is on the left of the card, on either the front or the back (ISO 7816-2) [16]. Many of the cards also incorporate a magnetic stripe to be compatible with existing equipment . A sample of a smart card is given in Figure 2.5.



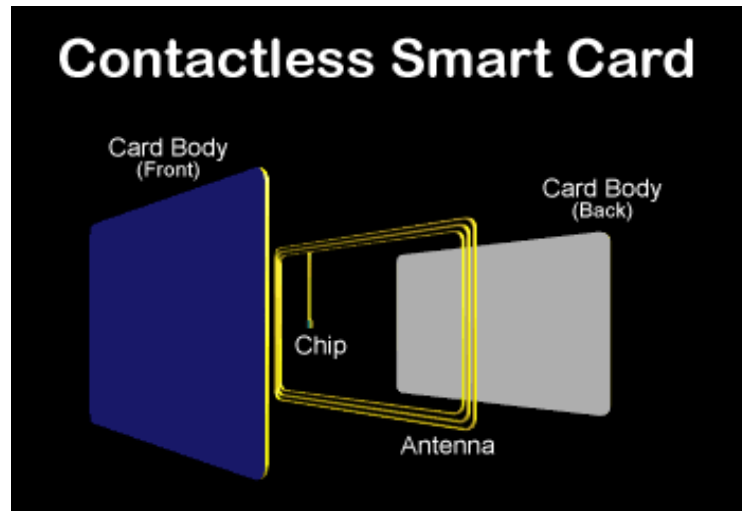
**Figure 2.5. Contact Smart Card**

The integrated circuit chip on a Smart Card requires some facilities fed to it from the outside world. Generally these are an electrical voltage to power the chip, a clock frequency to drive the chip and an input/output path for the transmission of data. The contact card achieves this through direct connections.

- ***Contactless Smart Cards (RF/ID and RF/DC)***

The contactless smart card dispenses with the contact plate on the surface of a smart card and instead uses some form of electrical coupling. Generally, contactless smart cards will be placed in close proximity to a reader, less than 3 centimeters. An inductive (transformer) or capacitive coupling is used to transfer energy and power the card. The clock may be internally derived and input/output is achieved by modulating the power signal.

There are several different processes that can accomplish this, including inductive coupling and capacitive coupling . Physical characteristics of a contactless smart card is given in Figure 2.6.



**Figure 2.6. Contactless Smart Card**

### ***Inductive Coupling***

Inductive coupling involves the use of two coils of wire - one acts as a primary coil and one acts as a secondary coil. An alternating current passes through a primary coil that creates an alternating magnetic field, which induces a flow of current in the secondary coil when they are in close proximity. Modulating the current at two different frequencies as it passes through the primary coil allows data to be transmitted to the secondary coil. When the card receives the current, it demodulates the signal and retrieves the data at the same time as it uses the transmitted power to activate its circuitry. Therefore, the advantage to this process is that it is able to transfer both information and power to a smart card .

### ***Capacitive Coupling***

Capacitive coupling involves placing a pair of conductors below the surface of the smart card. When a voltage signal is placed across them, a charge separation occurs that generates an electric field. The electric field can extend beyond the surface

and induce another charge separation on a second pair of conductors in the read/write unit, which transmits data between the card and the read/write unit [17]. The advantages to this technique are that digital information can be transferred directly and no modulation is required .

Some forms of contactless smart card operate at a longer distance and use radio wave energy. However, the power required of the radio waves to achieve this is often very high and most such radio systems use tokens with on board batteries, which means they are cannot conform to the correct physical dimensions (ISO 7816-1) and are therefore not proper smart cards.

Today's Contactless Smart Cards are defined by ISO 10536 which is a fairly loose standard since different manufacturers use different methods of coupling which are incompatible with one another. No two manufacturer's contactless smart cards are compatible at the coupling level. As technology improves, very low power chip and ultra thin batteries are becoming available, it is possible for the card to meet the smart card physical standards.

The following are some of the advantages of contactless cards over contact cards:

- Reliability: Surface contacts are usually where failures occur in electrical systems. Surface contacts on contact cards are susceptible to damage, contamination and wear, making failures more likely to occur.
- Longer Life: For the same reasons mentioned above.
- Facility: The contactless card can be placed in any orientation toward the read/write unit, whereas the contact card must be placed in a slot in a specific direction.
- Convenience: The read/write unit for contactless cards can be mounted under or behind any non-metallic working surface.
- Minimal maintenance: The read/write units have no moving mechanical parts, which requires minimal maintenance.
- Robustness: The read/write units and contactless cards can withstand harsh environments and weather. Therefore, they are suitable for use in industrial or

other harsh environments where they may come in contact with oil, grease or dirt.

Beside having a loose standard, current generation of contactless smart cards do have some other disadvantages. They tend to be rather slow and expensive to build and tend to fail as a result of flexing since they consist of a number of linked components rather than a single chip. Furthermore, there are also problems in embossing some types of contactless card since embossing damages the components. Potentially they are less secure as a result of the potential to couple a listening device at the card - reader air interface.

### ***Super Smart Cards***

The types of smart cards that have presented so far are considered as a passive card which required an external source of power supply and read/write terminal. This restriction inevitably affects their suitability for certain types of application. For instance, any passive smart card system must ensure adequate terminal availability throughout the planned area of the service (Roy Bright 1988). This led to the development of the third generation active smart card, known as Super Smart Card, which is currently under development.

Super Smart Card incorporates a keyboard and display directly on the surface of the card. It can function as a standalone unit, or connect to a computer. For this purpose, they also generally have surface contacts. Disadvantages to the super smart card include the high cost of production in comparison with the other cards, the difficulty in meeting ISO standards and the small size of the keypad .

The primary benefit of a Super Smart Card (active card) is its off-line, self-validating functionality. Unlike terminal-power passive cards, it is usable at any time in any location, yet, with its built-in PIN-validating programmes and other secure features, access is as highly protected as any existing smart card system (Roy Bright 1988).

As this card is still under development, no standard has yet been formulated for this new generation of card.

## *Classification of Smart Card*

The integrated circuit chip may simply contain memory, it may be controlled by some hardwired logic, for example offering PIN controlled access security, or it may contain a microprocessor. Depending on their communication methods (ISO 7816-3), Smart Cards can further be classified as Intelligence or Memory Cards [18].

- **Intelligence Smart Card (Asynchronous Card)**

The intelligence smart card contains a memory module and a Central Processing Unit (CPU) with the abilities to store and secure information, the power to make decisions and read/write capabilities.

In the case of a card housing a microprocessor, once powered and interfaced to a reader, to all intents and purposes, the chip on the card is a full blown computer. It is operating under control of an operating system also housed on the chip known as Smart Card Operating System (SCOS), which is unique to the chip or card supplier. The SCOS is also known as Reader Operating System (ROS).

Given this capability, it is possible to drive the input/output line between the smart card and the reader as though it were a normal RS232 communications line. ISO 7816-3 defines a communications mechanism similar to RS232 operating at 9600 baud with even parity. ISO 7816-3 goes one stage further and considers the nature of the traffic and protocol across the link. ISO 7816-3 T=0 defines the nature of the messages and responses across the communications link on a character by character basis.

The character by character nature of the standard creates a number of problems in that, if an error occurs in a message, it is difficult to know what to re-transmit and which of the received or transmitted data is correct. This problem was resolved by extending the standard to ISO 7816-3 T=1 which defines a block protocol by creating packets of the ISO 7816-3 T=0 messages. The T=1 format is very much better than the T=0 format in terms of transmission error resilience, but of course the underlying message response format remains unchanged and is still as bad in computer terms as mentioned above. Most processor smart cards on the market today



still operate under ISO 7816-3 T=0. The protocol used by processor cards is known as an Asynchronous protocol and one often hears talk about asynchronous cards which simply means cards housing a processor.

When a processor card is powered up and reset, it immediately sends a data stream to the reader, which identifies the chip type and details the nature of the protocol being used. This data stream is known as an Answer To Reset (ATR) string. Further detail about protocols will be discussed in the subsequent section.

- **Memory Smart Card**

The synchronous card is a purely memory storage card, that do not have the luxury of a microprocessor and operating system to control them.

Once linked to the outside world, they are powered, clocked and addressed totally under control of the outside world. All that it is possible to do is directly address the memory on the chip. Those non processor chips that have hard wired logic to control access security, operate simply by setting an internal on/off switch based upon an equal or not equal compare of supplied data (the PIN) with a hidden data area in the chip's memory. Once the test has been passed, the switch is set and data is accessible or updateable according to chip type.

In the case of a chip used in telephone cards and similar applications, the hard wired logic treats the chip memory as a counter by allowing one bits to be set to zero bits (or vice versa) but not the reverse. Bits may be treated as individual bits to be counted or in groups to form octal or hexadecimal numbers.

Regardless of whether there is any hardwired logic or not, the operation of accessing chip data and performing input/output operations is under control of the host. ISO 7816-3 defines very little in this area, in fact all it does is to define the location and format of a base identifying code for the chip type. In addition, each manufacturer implements its chips in different ways; in fact, each chip from each manufacturer chip tends to be implemented in a different way. This means that if a smart card of unknown type is placed into a smart card reader, one has to proceed through a series of trail and error exercises.

For example, the host software driving the reader will carry out the following tests. Is the card loaded a processor card? If yes then an Answer To Reset (ATR) will be received by the reader and the rest is easy. If this is not the case then it must be assumed that the card is a non-processor card. And now the problem starts since it is not just a matter of reading the identifying byte. Before that can be achieved, the correct mechanism for talking to the chip must be adopted. All the reader can do is to try different methods until a response is received. Once a response is received, then the communication mechanism is assumed to be correct and the chip identifying code can be read.

In practice this means that in general, with non-processor cards, all card types that may be used in an environment must be known in advance and supported.

### **2.1.6. CombiCard**

The CombiCard is a single card which has the features of both contact and contactless smart card with addition of magnetic strip, 2-dimensional and/or one-dimensional bar code technology incorporated into the card. This allows the card to be multi-applicational if necessary. Physical characteristics of a combi card is given in Figure 2.7.

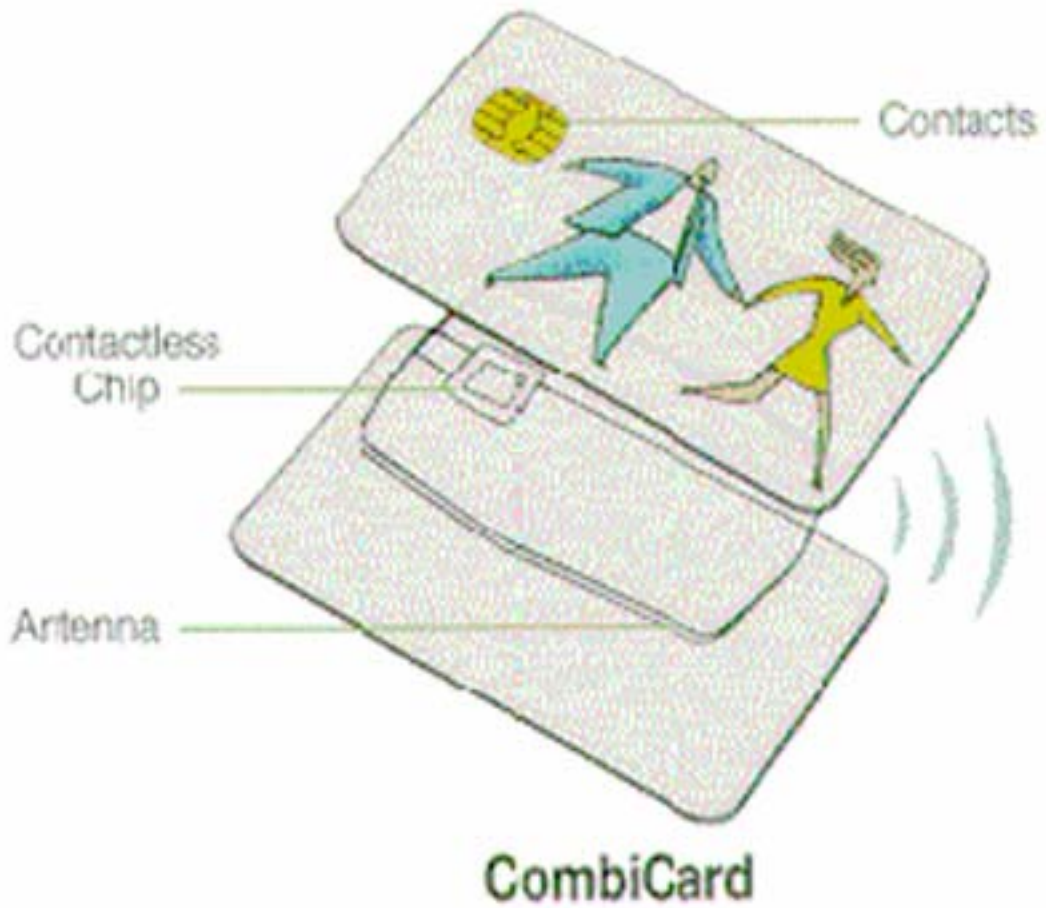


Figure 2.7. CombiCard

## **2.2. E-Payment Architectures**

E-payment systems can be categorized into three different architectures according to the synchronization (data transfer) between pos terminals and the main server.

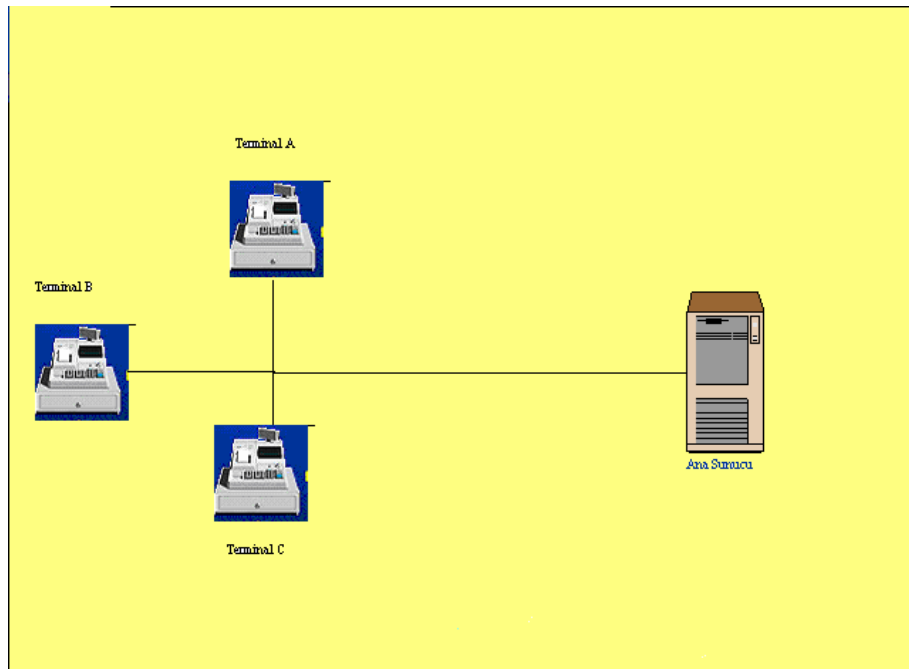
### **2.2.1. Online Systems**

In this architecture; all data are synchronized between the server and the pos terminals in real time. In other words, whenever a sale transaction occurs at the pos terminal, this information is immediately transferred to the server. There is always a network link between server and pos terminals. Online network architecture is given in Figure 2.8. There are some benefits of this architecture listed below:

- 1) You can see transaction data in real time.
- 2) In case of failure in one of the Pos terminal, you will not lose any data, because the because of the real time synchronization between the server and pos terminal.
- 3) It is easy to keep track network link down cases by developing pos terminal monitoring software, which increases also the security.
- 4) In this architecture, you do not have to store the credit value of the cardholder on the card used for e-payment. By storing the credit value on the server, you can check the current balance of the user from the server [19].

### **2.2.2. Semi-Online Systems**

In this architecture; all data are synchronized between the server and the pos terminals in an event-based manner. Those events maybe opening the shift, or closing the shift. In those systems, there are not always a network link between the pos terminal and a server. The data is synchronized by connecting to the server. A data transfer technique in which there is a special hardware (usb memeory stick, palm, etc) used for data synchronization can be used in this architecture also. In the case of transaction transfer between the server and vending machines, there can be palms



**Figure2.8. Online Working Systems**

used [20]. Semi online working systems architecture is given in Figure 2.9. There are some advantages and disadvantages of this algorithm listed below:

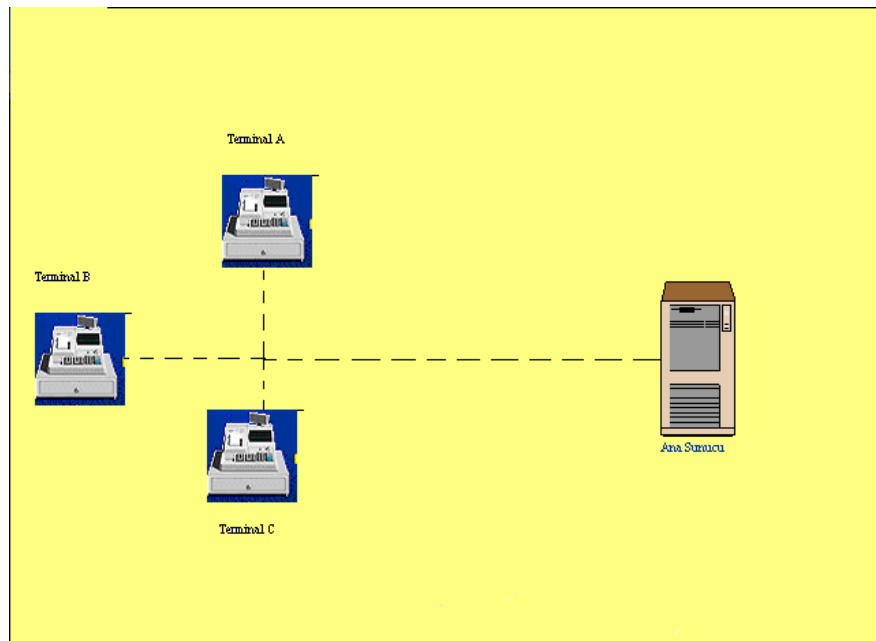
- 1) You can not see transaction data in real time.
- 2) In case of failure in one of the Pos terminal, you will lose data for a period of data transfer, because of the event-based synchronization between the server and pos terminal.
- 3) It is not easy to keep track pos out of order, because all pos terminals are not connected to the network.
- 4) In this architecture, you have to store the credit value of the cardholder on the card used for e-payment.

### **2.2.3. Offline Systems**

In this architecture; there is not network link between the pos terminals and the server. There is actually not a server on which the transaction data is stored. Pos terminals are working independently from each other. Data update (black list, white list, etc.) on the server can be done by special hardware such as usb memory stick,

palms, etc. There are some advantages and disadvantages of this algorithm listed below:

- 1) You can not see transaction data on the server.
- 2) In case of failure in one of the Pos terminal, you will lose all the data stored on the pos terminal.
- 3) It is not easy to keep track of pos out of order cases, because all pos terminals are not connected to the network.
- 4) In this architecture, you have to store the credit value of the cardholder on the card used for e-payment.



**Figure2.9. Semi-Online Working Systems**

## **CHAPTER 3**

### **SECURITY IN E-PAYMENT SYSTEMS**

In this chapter, first the security concepts will be explained. Then the e-payment system security will be examined under two topics. One is physical security and the other one is data security.

Security is one of the major issues in e-payment systems. With the introduction of the computer, the need for automated tools for protecting files and other information stored on the computer become evident. This is especially the case for a shared system, such as a time-sharing system, and the need is even more acute for systems that can be accessed over a public telephone network, or the internet. The generic name for the collection of tools designed to protect data and to thwart hackers is computer security [21].

With the introduction of distributed systems and with the use of networks and communication facilities for carrying data between terminal user and computer and between computer and computer, there has been a major issue raised for data transmission. Network security measures are needed for to protect data during their transmission [22].

There are no clear boundaries between these two forms of security. For example, one of the most publicized types of attack on information systems is the computer virus. A virus may be physically when it arrives on a diskette and is subsequently loaded on to a computer. Viruses may also arrive over an internet. In either case once the virus is resident on a computer system, internal security tools are needed to detect and recover from the virus.

The two main goals of security are to protect the data from unauthorized access, prevent modification of the data during its transmission. The goals of the security are given in Figure 3.1.

# Security Goals

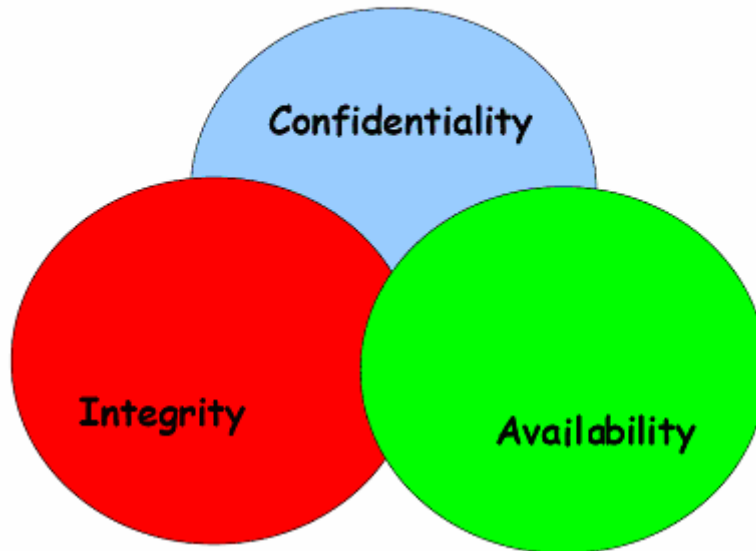


Figure 3.1. Goals of Security

## 3.1. Security Concepts

To assess the security needs of an organization effectively and to evaluate and choose various security products and policies, the manager responsible for security needs come systematic way of defining the requirements for security and characterizing the approaches to satisfy those requirements. One approach is to consider three aspects of information security:

- **Security Attack:** Any action that compromises the security information owned by an organization.
- **Security Mechanism:** Any mechanism that is designed to detect, prevent, or recover from a security attack.
- **Security Service:** A service that enhances the security of the data processing systems and the information transfers of an organization.



- **Interruption:** An asset of the system is destroyed or becomes unavailable or unusable. This is an attack on availability. Examples include destruction of a piece of hardware, such as a hard disk, the cutting of a communication line or the disabling of the file management system.
- **Interception:** An unauthorized party gains access to an asset. This is an attack on confidentiality. The unauthorized part could be a person, a program, or a computer.
- **Modification:** An unauthorized part not only gains access to but also tampers with an asset. This is an attack on integrity. Examples include changing values in a data file, altering a program so that it performs differently, and modifying the content of messages being transmitted in a network.
- **Fabrication:** An unauthorized party inserts counterfeit objects into the system. This is an attack on authenticity. Examples include the insertion of spurious messages in a network or the addition of records to a file.
- **Confidentiality:** Confidentiality is the protection of transmitted data from passive attacks.
- **Authentication:** The authentication is concerned with assuring that a communication is authentic. In the case of a single message, such as a warning or alarm signal, the function of authentication service is to assure the recipient that the message is from the source that it claims to be.
- **Integrity:** Ensuring that information is not altered by unauthorized persons in a way that is not detectable by authorized users
- **Access control:** Ensuring that users access only those resources and services that they are entitled to access and that qualified users are not denied access to services that they legitimately expect to receive

- **No Repudiation** : Ensuring that the originators of messages cannot deny that they in fact sent the messages
- **Availability**: Ensuring that a system is operational and functional at a given moment, usually provided through redundancy; loss of availability is often referred to as "denial-of-service"

## Security Attacks

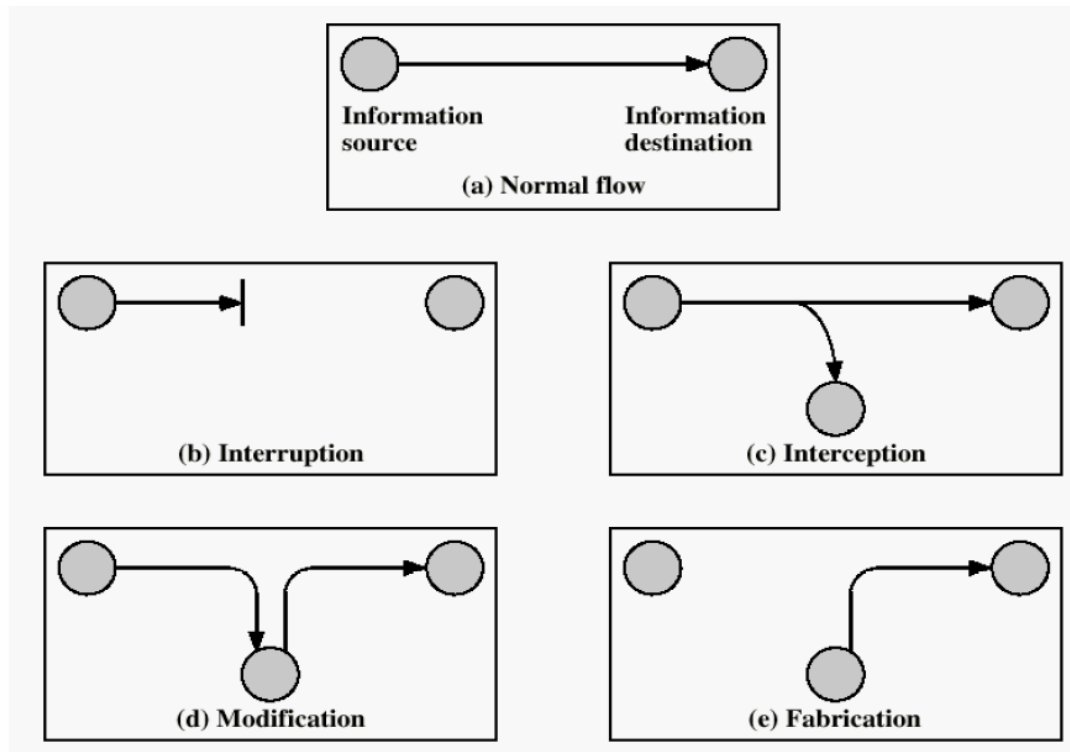
Different types of security attacks are shown in the figure 3.1. Attacks can be categorized into two categories as passive and active attacks:

**Passive Attacks:** Passive attacks are in the nature of eavesdropping on or monitoring of transmissions. The goal of the opponent is to obtain information that is being transmitted. Two types of passive attacks are, release of message contents and traffic analysis.

- **Release of message content:** It is self explanatory with its name. A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information. We would like to prevent the opponent from learning the contents of these transmissions.
- **Traffic analysis:** Analysis of the transmitted messages and try to get the information from the data sent through the transmission channel.

**Active Attacks:** The second major category of attack is active attacks. These attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories: masquerade, replay, and modification of messages and denial of service. Security attack types are given in Figure 3.2 [22].

- **Masquerade:** Masquerade takes place when one entity pretends to be a different entity. A masquerade attack usually includes one of the other forms of active attack. For example, authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling



**Figure3.2. Security Attacks**

an authorized entity with few privileges by impersonating an entity that has those privileges.

- **Replay:** Involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.
- **Modification of Messages:** It means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect.
- **Denial of Service :** Prevents or inhibits the normal use or management of communications facilities. This attack may have a specific target; for example, an entity may suppress all messages directed to a particular destination. Another form of service denial is the disruption of an entire network, either by disabling the network or by overloading it with messages so as to degrade performance.

### **3.1.1. Physical Security**

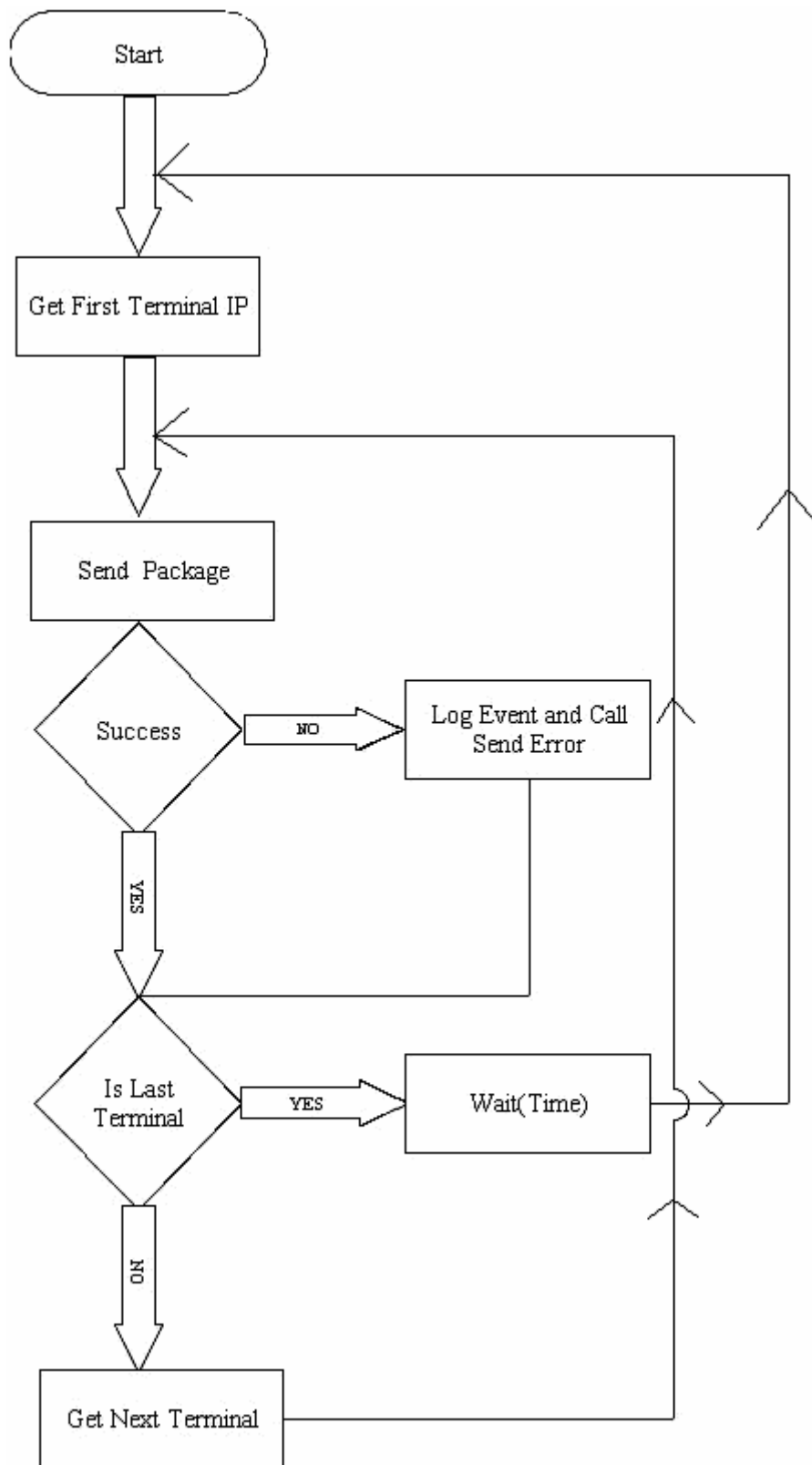
Physical security means protecting your hardware from unauthorized access. The above definitions are valid for data security. Physical security is related to save your hardware. In this part, there are three different security parts will be examined. In the first part, the terminal monitoring software architecture will be introduced. In the second part, three tiered application layering and physical security will be examined. In the last part, the network architecture will be proposed for physical security.

### **3.1.2. Terminal Monitoring Software**

In online e-payment systems, there is always a network connection between main server and each terminal. To monitor and keep track the network link downs and any physical attempts to the end terminal either by an operator using the terminal or a third party person, a terminal monitoring software can be developed. With this software, you can easily control and track the any link down cases between the server and terminal. The terminal monitoring software should have the following functions:

- Terminal status control function
- Send Errors function

Terminal Status Control Function: This function sends packages to each an every terminal connected to the server periodically and logs the results. If any errors have occurred during the control, it logs the result and calls the send errors function. With this way, you can always check what is going on between your server and terminal. A flow chart for this function is given in figure 3. Terminal status function gets the IP addresses of the terminals from the server and sends packages. Flowchart diagram for terminal status function is given in Figure 3.3.



**Figure 3.3. Flowchart diagram for Terminal Status Function**

Send error function is the function that sends the error to the operator related to the relevant terminal. This function can send those messages as SMS or as an email. Through this way, you can easily keep track the any physical attempt to the terminals and easily take the required action on time.

### **3.1.2. Network Architecture**

There can be three different physical network architecture applied to the e-payment systems. One is open network, two is closed network and three is the modified open network architecture. In this part, those three network architectures will be examined and pros and cons will be listed.

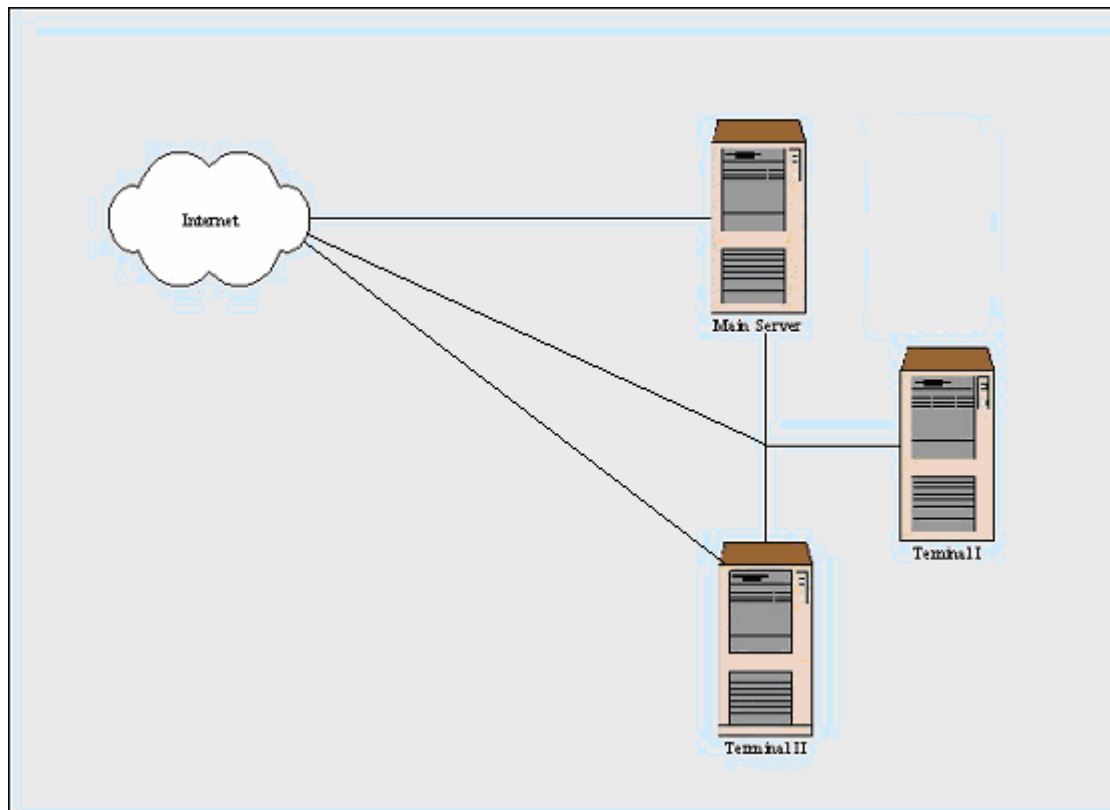
#### **Open Network Architecture**

In this architecture, server and all terminals have a network connection and those machines are in the public network of the campus or building. The Figure 3.4 represents this network architecture.

In this architecture system should be on behind of the firewall because the system is open to the threats. Through firewall you must configure and close the unused virtual ports. This network architecture is not very efficient to use in e-payment technologies.

#### **Closed Network Architecture**

In this architecture, the whole system is not open to the internet or intranet. It has its own private network and all terminals are connected to the server. Bu the server is not open to the internet. This architecture may be very efficient in the case of no needs for data to be accessed via web and all terminals can be connected to the server through the systems own network. But this architecture is not efficient, if real time access is needed to the system via web.

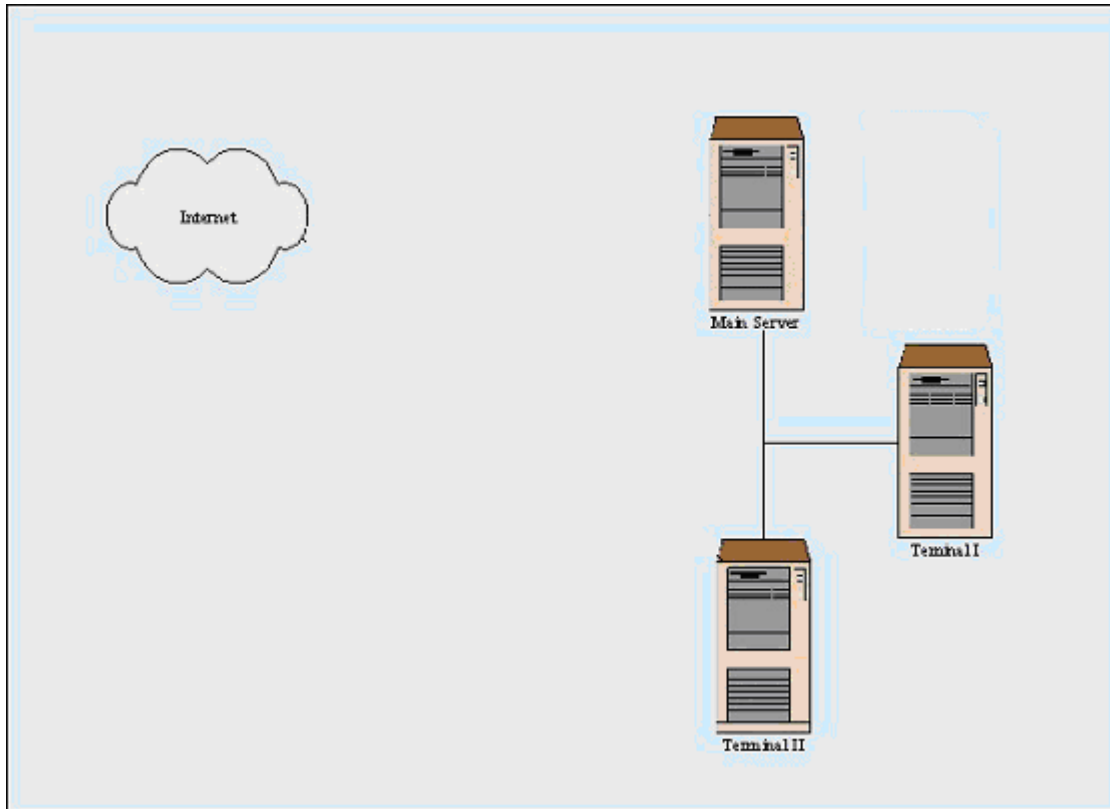


**Figure 3.4. Open Network Architecture**

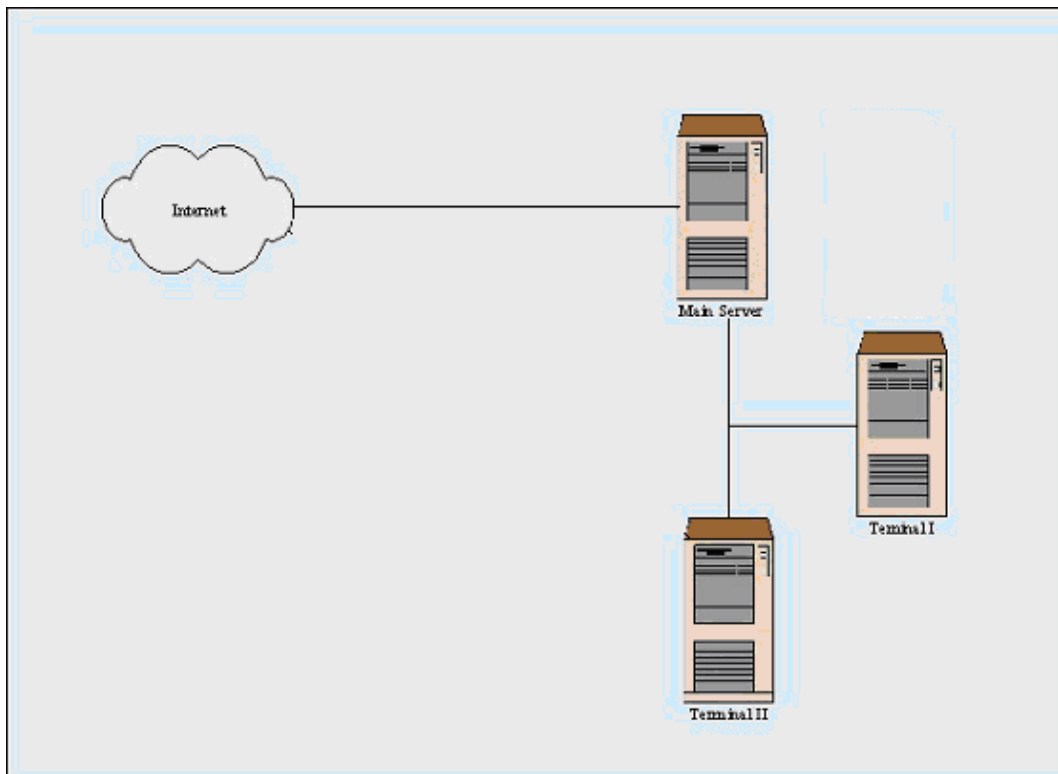
Figure 3.5 represents closed network architecture. This system is very safe regarding to the data security, but it is very inefficient to use.

### **Modified Open Network Architecture**

This architecture is very efficient to use and system data cannot be directly accessed via web. As shown in the Figure 3.6 data can be accessed via web though a web server, which has direct access to the database server. This reduces the threats to the database server and increases the data security. Among those three architectures, this architecture is the best to use. This architecture decreases the direct threats to the database server.



**Figure 3.5. Closed Network Architecture**



**Figure 3.6. Modified Open Network Architecture**



## 3.2. Data Security

### 3.2.1. Cryptography

The concept of *information* will be taken to be an understood quantity. To introduce cryptography, an understanding of issues related to information security in general is necessary.

Information security manifests itself in many ways according to the situation and requirement. Regardless of who is involved, to one degree or another, all parties to a transaction must have confidence that certain objectives associated with information security have been met. Some of these objectives are listed in Table 3.1.

**Table 3.1. Some Information on Security Objectives**

| <b>Concept</b>             | <b>Explanation</b>  |
|----------------------------|---|
| Privacy or confidentiality | Keeping information secret from all but those who are authorized to see it.                   |
| Data integrity             | Ensuring information has not been altered by unauthorized or unknown means.                   |
| Signature                  | A means to bind information to an entity.   |
| Authorization              | Conveyance to another entity of official sanction to do or be something.                      |
| Validation                 | A means to provide timeliness of authorization to use or manipulate information or resources. |
| Certification              | Endorsement of information by a trusted entity.   |
| Timestamping               | Recording the time of creation or existence of information                                    |
| Receipt                    | Acknowledgement that information has been received.   |
| Confirmation               | Acknowledgement that services have been provided  |
| Anonymity                  | Concealing the identity of an entity involved in some process                                 |
| Revocation                 | Retraction of certification of authorization  |

Over the centuries, an elaborate set of protocols and mechanisms has been created to deal with information security issues when the information is conveyed by physical documents.

Often the objectives of information security cannot solely be achieved through mathematical algorithms and protocols alone, but require procedural techniques and abundance of laws to achieve the desired result. For example, sealed envelopes delivered by an accepted mail service provide privacy of letters. The physical security of the envelope is, for practical necessity, limited and so laws are enacted which make it a criminal offense to open mail for which one is not authorized. It is sometimes the case that security is achieved not through the information itself but through the physical document recording it. For example, paper currency requires special inks and material to prevent counterfeiting. Conceptually, the way information is recorded has not changed dramatically over time. Whereas information was typically stored and transmitted on paper, much of it now resides on magnetic media and is transmitted via telecommunications systems, some wireless. What has changed dramatically is the ability to copy and alter information. One can make thousands of identical copies of a piece of information stored electronically and each is indistinguishable from the original. With information on paper, this is much more difficult. What is needed then for a society where information is mostly stored and transmitted in electronic form is a means to ensure information security which is independent of the physical medium recording or conveying it and such that the objectives of information security rely solely on digital information itself.

One of the fundamental tools used in information security is the signature. It is a building block for many other services such as non-repudiation, data origin authentication, identification, and witnessing, to mention a few. Having learned the basics in writing, an individual is taught how to produce a handwritten signature for the purpose of identification. At contract age the signature evolves to take on a very integral part of the person's identity. This signature is intended to be unique to the individual and serve as a means to identify, authorize, and validate.

Achieving information security in an electronic society requires a vast array of technical and legal skills. There is, however, no guarantee that all of the information security objectives deemed necessary can be adequately met. The technical means is provided through cryptography.

*Cryptography* is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication. Cryptography is not the only means of providing information security, but rather one set of techniques.

## **Ingredients of Cryptography**

**Plaintext:** This is the original message or data that is fed into the algorithm as input.

**Encryption Algorithm:** The encryption algorithm performs various substitutions and transformations on the plaintext.

**Secret Key:** The secret key is also input to the algorithm. The exact substitutions and transformations performed by the algorithm depend on the key.

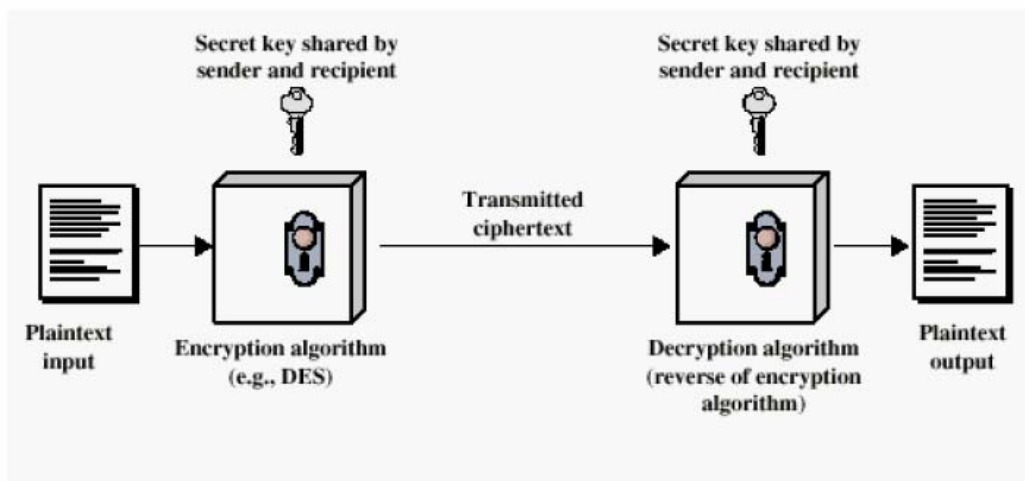
**Ciphertext:** This is the scrambled message produced as output. It depends on the plaintext and secret key. For a given message, two different keys will produce two different ciphertexts.

**Decryption Algorithm:** This is essentially the encryption algorithm run in reverse.

There are two types of encryption algorithms regarding to the keys that are used in the encryption and decryption; namely public key encryption and private key encryption algorithms.

### **Private Key Encryption Algorithms (Symmetric Encryption Algorithms)**

In symmetric key encryption algorithms, both receiver and sender use the same encryption algorithm and also same key. Figure 3.7 shows conventional or symmetric encryption algorithm structure [22].



**Figure 3.7. Private Key Encryption**

There are two requirements for secure use of symmetric encryption:

- 1) We need a strong encryption algorithm.
- 2) Sender and receiver must have obtained the copies of the secret key in a secure fashion and must keep the key secure.

Example conventional encryption algorithms are Data Encryption Standard (DES), Advanced Encryption Standard (AES) and so on.

One of the major issues in conventional encryption algorithms is key distribution. Key distribution can be done in one of the following ways:

- 1) A key is selected by sender and physically delivered to the receiver.
- 2) A third party could select a key and physically deliver it to both sender and receiver.
- 3) Sender may send the new key by encrypting new key using the oldest key used in data transmission.
- 4) A third party can encrypt the key and send both to receiver and sender.

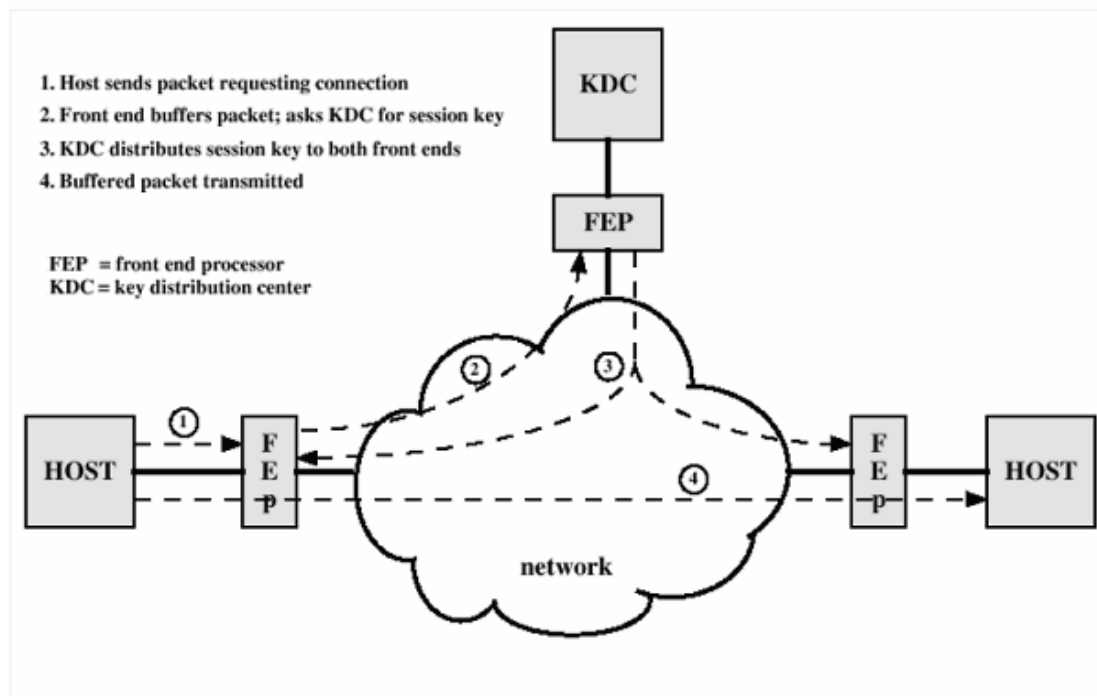
For the key distribution the followings should be identified.

**Session Key:** When two end-to-end systems wish to communicate, they establish a logical connection. For the duration of that logical connection, all user data are encrypted with a one-time session key.

**Permanent Key:** A permanent key is used between entities for the purpose of distributing session keys.

**Key Distribution Center:** Key distribution center determines which systems are allowed to communicate with each other.

Figure 3.8 shows automatic key distributor for connection-oriented protocol [22].



**Figure 3.8. Automatic Key distribution for Connection Oriented Protocol**

### **Public Key Encryption Algorithms (Asymmetric Encryption Algorithms)**

An encryption standard that uses two keys -- a *public key* known to everyone and a *private* or *secret key* known only to the recipient of the message is called public key encryption. When sender wants to send a secure message to receiver, he uses receiver's public key to encrypt the message. Receiver then uses her private key to decrypt it.

An important element to the public key system is that the public and private keys are related in such a way that only the public key can be used to encrypt messages and only the corresponding private key can be used to decrypt them. Moreover, it is virtually impossible to deduce the private key if you know the public key.

Public-key systems, such as Pretty Good Privacy (PGP), are becoming popular for transmitting information via the Internet. They are extremely secure and relatively simple to use. The only difficulty with public-key systems is that you need to know the recipient's public key to encrypt a message for him or her. What's needed, therefore, is a global registry of public keys, namely key distribution center. Public key encryption algorithm is shown in Figure 3.9.

Public key cryptography was invented in 1976 by Whitfield Diffie and Martin Hellman. For this reason, it is sometime called *Diffie-Hellman encryption*. It is also called *asymmetric encryption* because it uses two keys instead of one key (*symmetric encryption*).

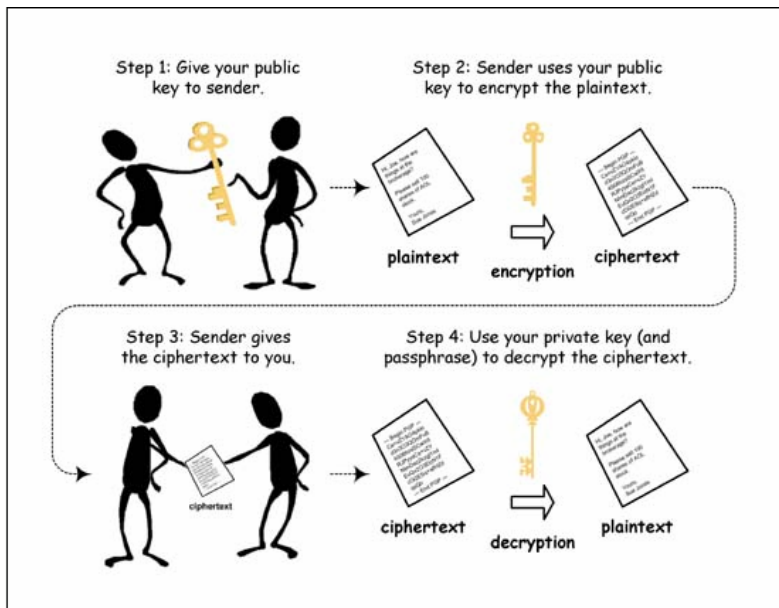
In summary the public key and private key encryption algorithms are compared in the following section.

- Traditional secret key cryptography uses a single key shared by both sender and receiver
- If this key is disclosed communications are compromised
- Also does not protect sender from receiver forging a message & claiming is sent by sender, parties are equal

**Public-key (or two-key) cryptography** involves the use of two keys:

A **public-key**, which may be known by anybody, and can be used to **encrypt messages**, and **verify signatures**.

A **private-key**, known only to the recipient, used to **decrypt messages**, and **sign (create) signatures**.



**Figure 3.9. Asymmetric Encryption System**

The public-key is easily computed from the private key and other information about the cipher (a polynomial time (P-time) problem) however, knowing the public-key and public description of the cipher, it is still computationally infeasible to compute the private key (an NP-time problem) thus the public-key may be distributed to anyone wishing to communicate securely with its owner (although secure distribution of the public-key is a non-trivial problem - the **key distribution** problem).

Public key and private key encryption algorithms may be used for network security. Public key encryption algorithms may be used for message authentication and digital signatures. Those standards are used for data security [23].

### 3.2.2. E-payment Mean Security

Depending on e-payment systems, some information related to the owner of the e-payment are stored on those means. It should not be easy to decode, read and modify the data stored in those cards. Some means use some physical switch security techniques for you to read data, whereas others supports some cryptographic standards such as DES, 3DES to store data. The data on the e-payment mean should

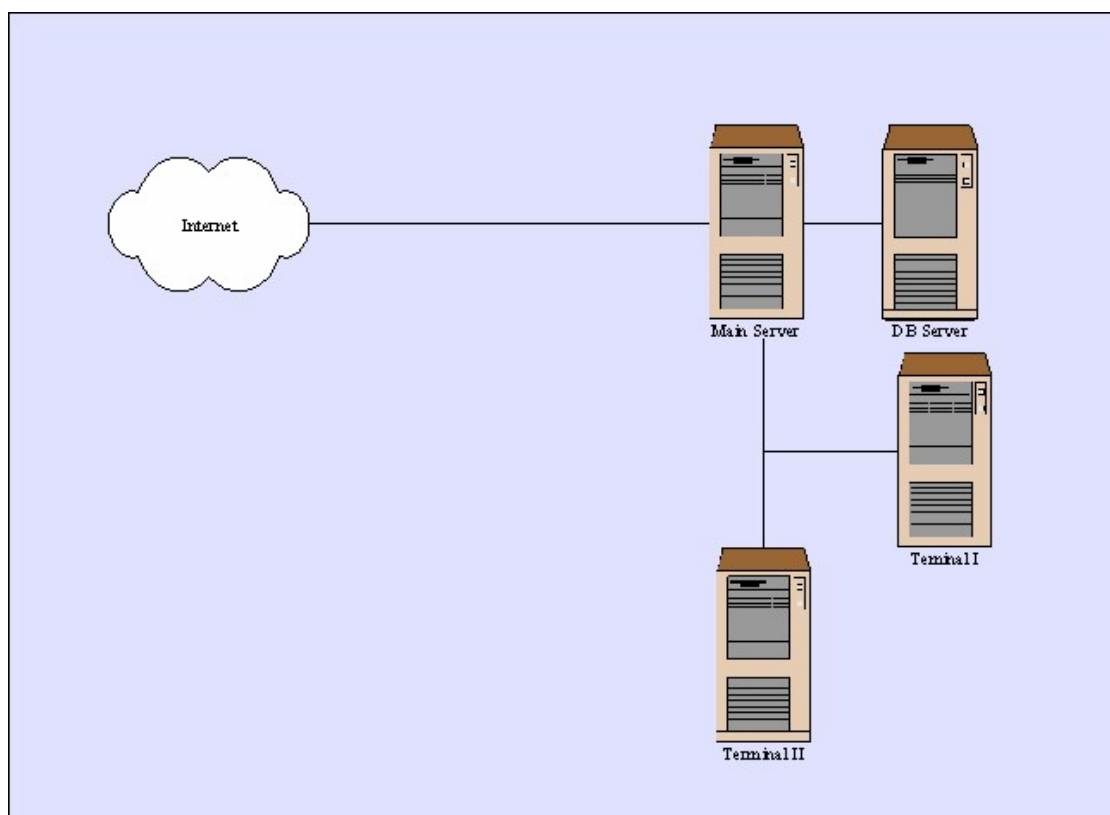
not be read and modified for the system not to be broken. The mean also should not be easily reproduced and used in the terminals of the e-payment system [24].



## CHAPTER 4

### PERFORMANCE IN E-PAYMENT TECHNOLOGIES

High performance is one of the nonfunctional requirements for e-payment systems, which should be satisfied for maximum utilization from the system. There is a strong and often network communication between the end terminals and the main server as shown in the following figure in e-payment systems.



**Figure 4.1. Network Architecture for E-Payment System**

There is a high network traffic between the server and terminals. This traffic is due to the transaction, blacklist and other information transfer. There are two different techniques can be used to real time transfer data between POS terminals and main server. Those techniques are given below.

- 1.Polling
- 2.Handshaking

The following section will explain those techniques.

#### **4.1 Polling Based Systems**

In those systems, POS terminals send data to the main server and also updates some information such as black list in their local database themselves. In such systems sending information may not be easy. Following scenarios can occur during data transfer.

1. Main server may not be online. In this case POS terminal will make polls to the main server which will cause performance degrade in terminals for nothing. In such systems the out of ten data transfer polls returns without a transfer[25].
2. The main server maybe online but the network link failure may take place. This will also cause communication failure between the server and POS terminal. In case of polling for data transfer, POS terminal will be try to send data to the server till success. This will also cause a performance degrade on POS terminal.
3. Both terminal and server may be online, but during data transfer the connection may be broken. This also requires more polls for the data to transfer from terminal to the server which degrades the performance of the POS terminal.

As can be seen from the above scenarios, polling is a time consuming process. It also creates junk traffic in the network which yields performance degrade in whole network.

#### **4.2 Handshaking Based Systems**

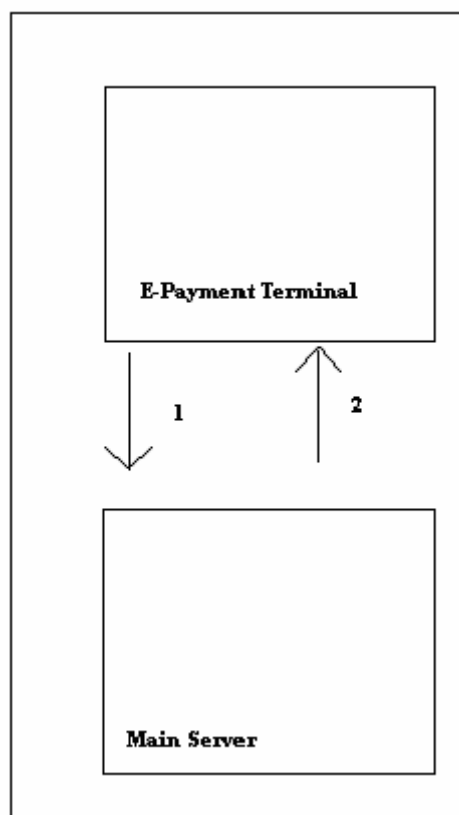
The performance measure mentioned in this work is increasing the performance by replacing polling with handshaking method. Process diagram of handshaking method is given in the figure 4.2. The communication between terminal database server and main database server is done using RPC calls. There is already a heavy traffic on in the network of e-payment systems because of the high transaction capacity of such

systems. The general trend for data transfer between the terminal and server is polling method, which degrades the performance of the terminal.

The disadvantage of polling is to make call at each time interval, even there is no message created on database server [26]. According to the statistics the nine polls out of ten returns no message. In other words there is no message created for students in the message table for nine polls out of ten.

To prevent this performance decrease, we introduce a new method called handshaking method. The stages of this method as shown in the Figure 1 are:

- 1) When a transaction takes place on the terminal of the e-payment system, the e-payment system makes RPC call with the appropriate message parameters to the main server for the data transfer to the server.
- 2) After the server grants the request, it makes RPC to the terminal to transfer that data to the main server. The RPC request is deleted at the server.



**Figure 4.2. Handshaking Process Diagram**

The pseudo code for automessage is given in Figure 4.2[27].

```
    Create_Message_On_Main_DB(id,msg)
    Trans_call_request(id,userid)
    Response_Trans_call(id,userid)
    If trans_found=true then
        Request_delete_from_db(id)
        Transfer_trans_to_server(id,userid)
    else
        ignore_request()
    End if
```

**Figure 4.3. Pseudo code for transaction transfer from terminal to server**

#### **4.2.1. Data Loss in Handshaking Method**

Another benefit of handshaking solution is related to the data loss in e-payment systems. Transactions in e-payment systems are most valuable data that is to be kept tracked to show the owner of the payment means their spendings. In polling based systems, data from the terminal is send to the main server in the defined polling intervals. If there is a crash occurs in the disk of the terminal before the transaction data is transferred to the server, the transaction data is lost. In handshaking based payment systems, transaction data is transferred just after the transaction takes place.

## CHAPTER 5

### APPLICATION OF SECURITY AND PERFORMANCE

#### ARCHITECTURES

The application of proposed security and performance architectures will be explained in this chapter. The example application *Pay ON-LINE* [20] will also be introduced in this chapter.

##### 5.1. Pay ON-LINE: Example Application

Pay ON-LINE is e-payment system of IŞIK University. Students and staff use this system for their payments at the Şile Campus of the university. There are subcontractors at different locations of Campus. They also use this system for their payments from the University and for electronic payment purposes.

There are more than 2000 users of the system, which are, grouped into 4 different user groups. As development technology, *ASP .Net* is used with *MS SQL Server 2000* as database management system. For windows applications run on POS terminals *Visual Basic .Net* technology is used.

The *Design Specification Document* of Campus ON-LINE is attached to this document at Appendix A. System terminals, user types and modules are also explained in Appendix A.

##### 5.2 Security Architecture of Pay ON-LINE

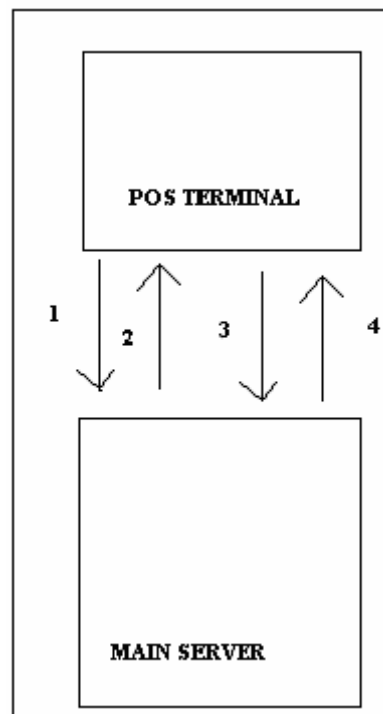
Pay ON-LINE is composed of actually terminals and web interfaces for reporting and administrative purposes. The security architecture explained above sections is the use of cryptography for network security. Security issues are explained in three different sections.

The explained security architecture above is the use of cryptography during data transfer on the network. This is needed for the *sniffers*, who listens your network,

may alter the content, or reproduce the content. Cryptography is also used in data security during transfer from terminal to the server.

Pay ON-LINE uses SSL certificate for web interfaces. Secure Socket Layer is used to encrypt the data during data transfer on the network for web based applications. Unexpected network listeners may not understand any package content on the current network.

For the POS terminals Pay ON-LINE uses its own encryption mechanism. Server and POS terminal negotiate on a key and algorithm. The algorithm is selected arbitrarily not to be broken. The process is explained and given in figure 5.1.



**Figure 5.1. Process diagram for key exchange and data transfer**

The above figure shows the data transfer phase between the POS terminal and main server. The stages are explained below:

- 1) POS terminal has requested a key and an algorithm from the server to encrypt the current data with the given parameters.
- 2) Server generates arbitrarily the method and key and sends it to the POS terminal.

3) POS terminal encrypts the data with the given parameters from the server and request a message pass to the server.

4) Server grants the request and takes the message and decrypts the data and stores in the main database.

For the physical security, main servers are placed in a safe room to which only the administrator's of Pay ON-LINE enter to this room. Beside this, a firewall is configured to catch DoS type of attacks, and all unused ports of the system are closed.

For network security, Pay ON-LINE POS terminals are isolated from the current network and it uses its own network. Only the web server can be reached in the current network, because presents the reporting and administrative functions of Pay ON-LINE.

Pay ON-LINE has a terminal monitoring software that monitors the system's terminals real time. If there is unexpected shut down occurs, or network link failure takes place, it send and sms and e-mail to the system administrators. The terminal monitoring software interface is given in Figure 5.2.

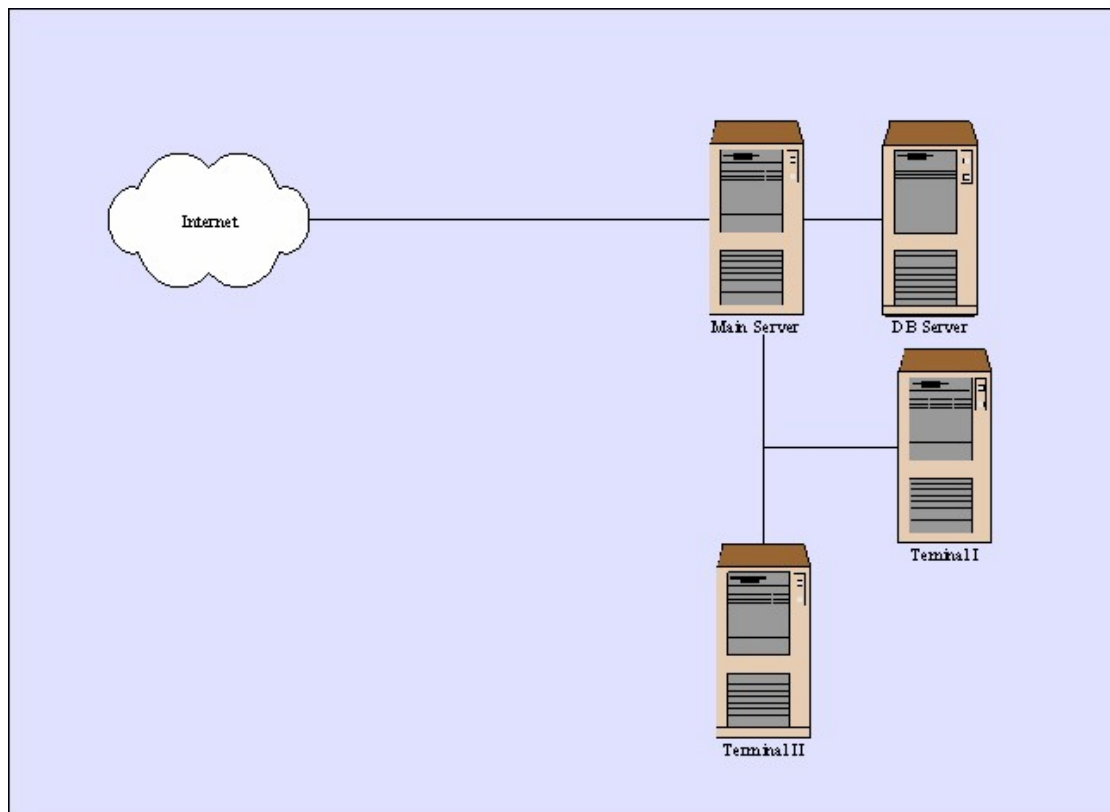
| Pay ON-LINE Terminals |                       |            |                       |
|-----------------------|-----------------------|------------|-----------------------|
| Terminal ID           | Terminal Name         | Ip Number  | Status                |
| 1                     | Leisure Center        | 10.150.2.2 | down                  |
| 2                     | Market                | 10150.2.1  | Un expected Shut down |
| 3                     | Dining Hall           | 10.150.2.3 | up                    |
| 4                     | Manual Loading Center | 10.150.2.4 | down                  |

**Figure 5.2. Terminal Monitoring Software**

Again related to the data security, any change on the server that is to be reflected to the POS terminals is JIT reflected. This is very important in the case of stolen cards. If the card is stolen and the administrator is made aware from this situation, the card is taken into the black list. This information is sent to all online terminals and others when they become first online. At the first POS terminal the card is blocked and the current operator of Pay ON-LINE reports the user.

Pay ON-LINE has two different servers. One is for database server, and one is for web server. The database server and the web server has direct link to each other but the database server is not directly linked to the network. The network architecture of Pay ON-LINE is given as below.

Pay ON-LINE uses smart cards as a mean. As mentioned above sections, smart card is the most accepted, secure mean for payment systems.



**Figure 5.3. Network Architecture of Pay ON-LINE**

### **5.3. Performance Architecture Of Pay ON-LINE**

For performance increase, Pay ON-LINE uses handshaking methodology replacing polling. Handshaking methodology and its performance increase are explained in the former sections. Pay ON-LINE uses this methodology for data transfer between the POS terminal and server. When the data is ready at the terminal side, terminal sends a request (RPC) for data transfer to the server with the right message parameters. When the server takes that request, it immediately process it and successfully transfer data from the terminal to the server.



This does not cause any junk traffic like in the polling based systems, and degrade the performance. Also, terminal is not dealing with the data transfer problem; it only deals with POS transactions. Server is responsible from the data transfer from the POS terminal to the server.

### 5.3.1. Performance Statistics

Before the polling based methodology, data transfers made by the terminal in Pay ON-LINE. Time based polling was made in Pay ON-LINE. Data transfer is done in ten minutes time based. During that time, the POS terminal is heavily dealing with the data transfer. The machine becomes unavailable changing from one to five minutes depending on the transaction amount. The metrics for CPU and MEM usage during transfer section is given in Table 5.1.

**Table 5.1 – Memory CPU usage during data transfer**

| <b>Parameter</b> | <b>Value</b>       |
|------------------|--------------------|
| CPU Usage        | %70 - %90          |
| MEM Usage        | 100-120 MB / 128MB |

In handshaking methodology, those degrades are not observed. Those jobs for the server in handshaking does transfer done by the terminals in polling based systems based systems.

## **CHAPTER 6**

### **CONCLUSIONS AND RECOMMENDATIONS**

In this thesis, E-Payment Systems are examined in security and performance areas. Some techniques and architectures are presented in this work.

First e-payment means that are to identify the mean owners in payment systems are examined. Depending on the requirements, some of those means can not be used. For example, if you would like your system to work offline, you must store the credit of the mean owner in the card. In that case, barcodes could not be used such systems. So, this technology is not applicable. Depending on the requirements, payment system developers must choose the appropriate mean.

The security of the payment systems are very important, because any change or intrusion to the system may cause unestimated results. You must use the security tools for network security, and data security in such systems. Phsical security of the servers are also important. You must choose the best network architecture for your system.

Performance of those systems are important, because any degrade in POS terminals will cause waiting of clerks, which is not acceptable.

In this thesis, a payment system which is the application of the security and performance architectures introduced above sections is developed. The project details on data definition, database diagram and modules, etc are given in appendix section. Some statistics on this system has taken and the results are reported above sections.

## REFERENCES

- [1] ECompany, <http://ecompany.ae/> ,May 30, 2006
- [2] Campus ON-LINE Web Site, <http://campus.isikun.edu.tr> ,June 03, 2006
- [3] Library ON-LINE Web Site, <http://library.isikun.edu.tr> , May 01,2005
- [4] Campus ON-SMS Web Site, <http://irdc.isikun.edu.tr/projects/campusonsms> ,  
July 05, 2005
- [5] *Mike Hendry*, Smart Card Security and Applications, Chapter 4 Card  
Technology, 2003
- [6] Barcode Island, <http://www.barcodeisland.com> , January 05,2006
- [7] *Mike Hendry*, Smart Card Security and Applications, Chapter 4 Card  
Technology, 2003
- [8] International Standards Organization, ISO 7811 Standard, <http://www.iso.org> ,  
February 10, 2006
- [9] ISO 14443, Identification cards, Contactless integrated circuit cards  
,Proximity cards, [http://www.iso.org/iso/en/prods-  
services/popstds/identificationcards.html](http://www.iso.org/iso/en/prods-services/popstds/identificationcards.html), June 03, 2006
- [10] Vijayan, J. and Brewin, B., 2003, “Walmart backs RFID technology,”  
Computerworld, June 16, 2003
- [11] K. Finkenzeller, RFID Handbook: Radio-frequency identification  
fundamentals and applications, Wiley, 1999.

- [12] ISO 7816, Smart Card Standard, <http://www.iso.org/iso/en/prods-services/popstds/.../en/StandardsQueryFormHandler.StandardsQueryFormHandler?languageCode=en&keyword=&lastSearch=false&title=true&isoNumber=7816&isoPartNumber=&isoDocType=ALL&ICS=&stageCode=&stageDate=&committee=ALL&subcommittee=&scope=CATALOGUE&sortOrder=ISO> , June 06 , 2006
- [13] W. Rankl, W. Effing , Smart Card Handbook, John Wiley and Sons, 2003
- [14] Smart Card Alliance, <http://www.smartcardalliance.org/> , March 14, 2006
- [15] ISO 15693. Identification cards – Contactless integrated circuit cards – Vicinity cards, <http://www.iso.org/iso/en/prods-services/popstds/.../en/StandardsQueryFormHandler.StandardsQueryFormHandler?languageCode=en&keyword=&lastSearch=false&title=true&isoNumber=15693&isoPartNumber=&isoDocType=ALL&ICS=&stageCode=&stageDate=&committee=ALL&subcommittee=&scope=CATALOGUE&sortOrder=ISO> , June 06, 2006
- [16] ISO 7816-2, Dimensions and location of the contacts, Smart Card Standard , <http://www.iso.org/iso/en/prods-services/popstds/.../en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=26536&ICS1=35&ICS2=240&ICS3=15> , July 01, 2006
- [17] K.P. Fishkin and S. Roy, Enhancing RFID Privacy via Antenna Energy Analysis, RFID Privacy Workshop, 2003,  
<http://www.rfidprivacy.org/papers/fishkin.pdf>
- [18] Zhiqun Chen, Java Card Technology for Smart Cards: Architecture and Programmer's Guide, Addison - Wesley, 2000
- [19] S. Kondakçı, An Approach to A National E-Payment Architecture, inet-tr, 2002
- [20] Pay ON-LINE, <http://pay.isikun.edu.tr> , January 20, 2006

- [21] E. Amoroso, Fundamentals of Computer Security Technology, Prentice Hall, 1994
- [22] W. Stallings, Cryptography and Network Security Principles and Practice, Prentice Hall, 2003
- [23] W. Stallings, Network Security Assentials Applications and Standards, Prentice Hall, 2000
- [24] Verifone,  
[http://bvcontent.verifone.com/VeriFone/Attachment/20040623/SAMs\\_WP.pdf](http://bvcontent.verifone.com/VeriFone/Attachment/20040623/SAMs_WP.pdf)
- [25] Karahasan O., Kuru S., “Gezgin Kullanıcıların Veritabanı Erişimi İçin Bir Başarım ve Güvenlik Yöntemi”, Bilgi Teknolojileri Kongresi IV, Denizli, 2006
- [26] Szallics K., *On Using the Observer Design Pattern*,  
<http://www.wohnklo.de/patterns/observer.html> , December 05, 2005
- [27] <http://www.mobilogren.com> , March 03, 2006

## APPENDIX A. DESIGN SPECIFICATIONS FOR PAY ON-LINE

In this section, design specifications of the example application are given. The description of database is done by describing the tables, describing the table definitions and with the Database diagram. The modules of the system will be listed with brief definitions.

| <b>A.1. Description of Database Tables</b> |  |
|--|--|
| <b>Table Name</b>                          | <b>Description</b>   |
| BlackList                                  | Table stores the cards that are in the black list for some reason.                                   |
| BlackListReasons                           | Stores the reason definitions of black list.   |
| BudgetDepts                                | Holds the departments of the spendings.  |
| CardEventDetails                           | This table stores (logs) the user events in the system.  |
| Cards                                      | Holds the e-payment mean information (smart card info). User relation is also done using this table. |
| CashMfillingWatcher                        | Holds the collection date, time and amount of banknotes in automatic loading machine.                |
| CashMLastCollectionDate                    | Holds the last collection date.  |
| CashMTransWatcher                          | Holds the transaction info in the automatic loading machine.   |
| Event_Types                                | Holds the event definitions of the system.   |
| Events                                     | Table stores the events of the users.  |
| LoadingDetails                             | Holds the credit card info for transactions.   |
| Old_Cards                                  | Holds the old card information and relation information with the user on it.                         |
| Shifts                                     | Stores the shift information of each terminal.   |
| SmartEvents                                | Holds the events of hand held devices that are used as pos terminal inside e-payment system.         |
| Subcontractor_Managers                     | Holds the subcontractor manager user information.  |
| Subcontractors                             | Holds the subcontractor information.   |
| Terminals                                  | Holds the terminal definitions including their IP, etc.  |
| Transactions                               | Stores the card transaction information, including terminal info, amount, etc.                       |
| User_Types                                 | Stores the user types of the system.   |
| Users                                      | Stores the user information of the system.   |
| VendPrices                                 | Holds Vending machine prices, required for data transfer from vending machines to the system.        |
| MealScholarship                            | Stores the meal scholarship information.   |

## A.2. Definitions of Database Tables

| Table                   | Column          | Type     | Length |
|-------------------------|-----------------|----------|--------|
| BlackList               | UserID          | char     | 10     |
|                         | DateTime        | datetime | 8      |
|                         | ReasonID        | int      | 4      |
| BlackListReasons        | ReasonID        | int      | 4      |
|                         | Description     | varchar  | 255    |
| BudgetDepts             | Department      | varchar  | 50     |
| CardEventDetails        | EventID         | int      | 4      |
|                         | CardID          | char     | 20     |
|                         | TerminalID      | char     | 10     |
| Cards                   | CardID          | char     | 10     |
|                         | UserID          | char     | 10     |
|                         | InsertionDate   | datetime | 8      |
| CashMFillingWatcher     | banknote        | int      | 4      |
|                         | counter         | int      | 4      |
|                         | datetime        | datetime | 8      |
| CashMLastCollectionDate | lastcollectdate | datetime | 8      |
| CashMTransWatcher       | transdate       | datetime | 8      |
|                         | CardID          | char     | 10     |
|                         | Amount          | money    | 8      |
| Event_ Types            | EventType       | tinyint  | 1      |
|                         | Description     | varchar  | 50     |
| Events                  | EventID         | int      | 4      |
|                         | OperatorID      | char     | 10     |
|                         | EventType       | tinyint  | 1      |
|                         | EventDate       | datetime | 8      |
|                         | TerminalID      | tinyint  | 1      |
|                         | Note            | varchar  | 255    |
| LoadingDetails          | TransID         | bigint   | 8      |
|                         | CCNumber        | char     | 16     |
|                         | TerminalID      | int      | 4      |
| Old_Cards               | UserID          | char     | 10     |
|                         | OldCardID       | char     | 10     |
|                         | CardExpireDate  | datetime | 8      |

|                        |                   |          |     |
|------------------------|-------------------|----------|-----|
|                        |                   |          |     |
| Shifts                 | OperatorID        | varchar  | 50  |
|                        | TerminalID        | varchar  | 50  |
|                        | Shift_Start_Date  | datetime | 8   |
|                        | Shift_End_Date    | datetime | 8   |
|                        |                   |          |     |
| SmartEvents            | EventID           | int      | 4   |
|                        | OperatorID        | char     | 10  |
|                        | EventType         | tinyint  | 1   |
|                        | EventDate         | datetime | 8   |
|                        | TerminalID        | tinyint  | 1   |
|                        | Note              | varchar  | 255 |
|                        |                   |          |     |
| Subcontractor_Managers | SubcontractorID   | char     | 4   |
|                        | UserID            | char     | 10  |
|                        |                   |          |     |
| Subcontractors         | SubcontractorID   | varchar  | 4   |
|                        | SubcontractorName | varchar  | 50  |
|                        | ResponsibleName   | varchar  | 100 |
|                        | Phone             | char     | 15  |
|                        | Fax               | char     | 15  |
|                        | Address           | varchar  | 100 |
|                        | Email             | varchar  | 30  |
|                        |                   |          |     |
| Terminals              | TerminalID        | int      | 4   |
|                        | Description       | varchar  | 255 |
|                        | Location          | varchar  | 50  |
|                        | IP                | char     | 15  |
|                        | Online            | bit      | 1   |
|                        | SubcontractorID   | char     | 4   |
|                        | TerminalType      | bit      | 1   |
|                        |                   |          |     |
| Transactions           | TransID           | int      | 4   |
|                        | CardID            | char     | 10  |
|                        | TerminalID        | int      | 4   |
|                        | OperatorID        | varchar  | 50  |
|                        | DateTime          | datetime | 8   |
|                        | TransactionAmount | money    | 8   |
|                        | FinalAmount       | money    | 8   |
|                        | Type              | smallint | 2   |
|                        | PType             | bit      | 1   |
|                        |                   |          |     |
| User_Types             | UserType          | int      | 4   |
|                        | Description       | varchar  | 50  |
|                        |                   |          |     |
| Users                  | UserID            | char     | 10  |
|                        | UserType          | int      | 4   |
|                        | User_Fname        | varchar  | 50  |
|                        | User_LName        | varchar  | 50  |



|                 |               |          |    |
|-----------------|---------------|----------|----|
|                 | Budget_Dept   | varchar  | 50 |
|                 | Campus        | varchar  | 50 |
|                 | InsertionDate | datetime | 8  |
|                 |               |          |    |
| VendPrices      | Type          | int      | 4  |
|                 | Price         | char     | 10 |
|                 |               |          |    |
| MealScholarship | CardID        | int      | 4  |
|                 | Amount        | smallint | 2  |



## A.4. Pay-ONLINE Terminals

There are 7 different terminals defined in Pay ON-LINE. They are listed below:

- i. Dining Hall
- ii. Market
- iii. Manual Loading Center
- iv. Automatic Loading Center
- v. Leisure Center
- vi. Youth Center
- vii. Vending Machines

Those terminals and their explanation are given in the following section.

### *i. Dining Hall*

Dining hall is a place in which all breakfasts, lunches and dinners are presented to both academic and non-academic personel(including students and staff). There is a Pay ON-Line terminal located at the dining hall of Işık University of Şile Campus. The interfaces and their definitions are given below:

First of all, to enter the system, operator must open a shift. Shift means the start and end period of transaction time for a valid operator. To open a shift, you must present a valid operator card. Shift information can be seen on the screen of the pos terminal. In this interface, you can see the special buttons only for dining hall interface. Those buttons are breakfast, lunch and dinner prices. Those prices are defined during the sign of a contract and entered to the system. You may change or lock the current shift. If you lock the current shift, you must present the locker operator card or the manager card to the system to unlock or close the current shift. On this screen, you may see the current card credits, transaction amount, and user information such as name, surname, and user type.

**Pay ON-LINE** Pay ON-LINE: Işık Üniversitesi Elektronik Ödeme Sistemi

Toplam 2,200,000  
Tahsil Edilen=1,200,000  
Fiş Tahsil Edilmiştir

Adı Soyadı Orhan Karahasna  
Kalan Kredi 97,800,000  
Kullanıcı Tipi Personel

Kartı Oku

Terminal Yemekhane POS  
Açılış Tarihi 26.02.2004 10:10:05  
Operatör Orhan Karahasnan

Kahvaltı Öğle Yemeği Akşam Yemeği

Tahsilat Tümü İptal Geri Al

Kilitle Vardiya Değiştir

Vardiya Raporu

GELİŞTİREN: ENFORMATİK UYGULAMA VE ARAŞTIRMA MERKEZİ

**Figure A.4.1. Dining Hall Operation Interface**

You may take shift report that shows the transaction information starting from the beginning of the shift till report time. The shift report interface is given below:

**Pay ON-LINE** Pay ON-LINE: Işık Üniversitesi Elektronik Ödeme Sistemi

Vardiya Bilgileri

| Kart Numarası | Yapılan Harcama Miktarı | Tarih               | Tipi          | Ödeme Şekli |
|---------------|-------------------------|---------------------|---------------|-------------|
| 231           | 750,000                 | 03.03.2004 15:35:29 | Kahvaltı      | Fiş         |
| 231           | 1,200,000               | 03.03.2004 15:35:30 | Muhtelif Gıda | Nakit       |
| 5             | 1,000,000               | 03.03.2004 15:37:19 | Kahvaltı      | Fiş         |
| 5             | 1,200,000               | 03.03.2004 15:37:19 | Muhtelif Gıda | Nakit       |

Terminal Yemekhane POS  
Açılış Tarihi 26.02.2004 10:10:05  
Operatör Orhan Karahasnan  
Kahvaltı Nakit:0-Fiş:2  
Öğlen Yemeği Nakit:0-Fiş:0  
Akşam Yemeği Nakit:0-Fiş:0  
Toplam Nakit İşlem 2,400,000

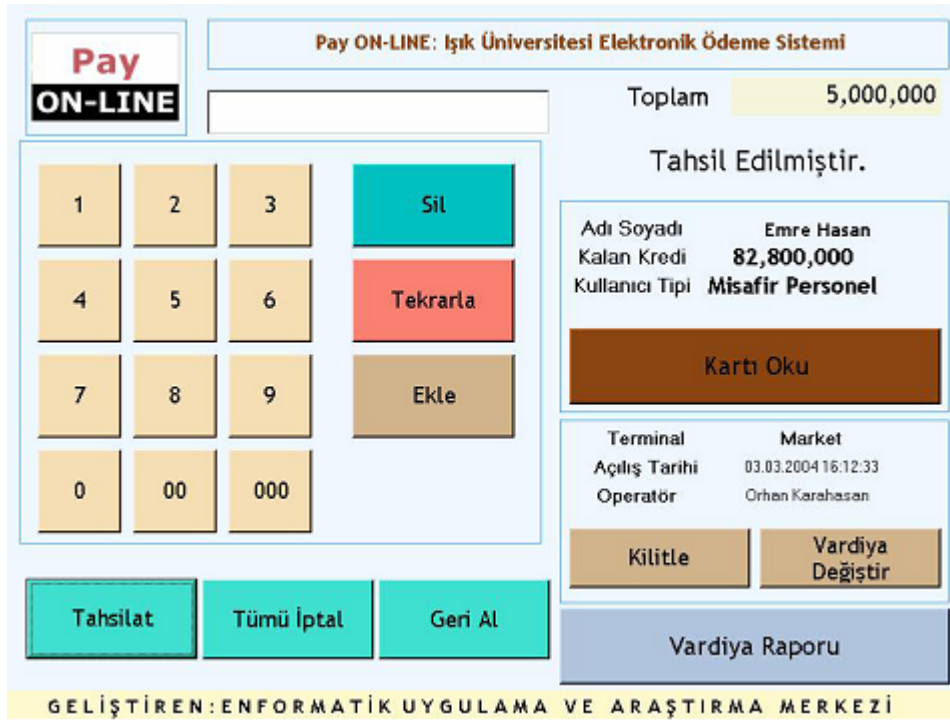
Tamam

**Figure A.4.2. Dining Hall Shift Report**

You may see the transaction type, total transaction amount, from the report. You may also see the current #of meal taken with cash, or with the scholarship. It also shows the shift information on it.

*ii. Market*

One of the Pay ON-LINE terminal is market. Market interface is not so different from the dining hall interface described above. The following interfaces are defined in the POS terminal of Market place in the campus.



**Figure A.4.3. Market Operation Interface**

As can be seen from the above interface, market POS terminal is composed of a simple calculator, spending buttons, card read buttons and lock and change shift buttons. It also has a functionality of shift report. It works with a basket. Each and every basket element may be cancelled or deleted from the basket. And you may also delete all elements in the basket using the “*Tümü İptal*” button. To change or lock the current shift, you must present the current operator’s card. Otherwise you could not complete this operation.

The report of Pay ON-LINE Market module is given below:



**Pay ON-LINE: Işık Üniversitesi Elektronik Ödeme Sistemi**

| Kart Numarası | Yapılan Hacama Mikta | Tarih               | Tipi           | Ödeme Şekli |
|---------------|----------------------|---------------------|----------------|-------------|
| 8             | 5,000,000            | 03.03.2004 16:12:42 | Muhzellif Gıda | Nakit       |
| 8             | 1,200,000            | 03.03.2004 16:12:48 | Muhzellif Gıda | Nakit       |
| 8             | 5,000,000            | 03.03.2004 16:16:15 | Muhzellif Gıda | Nakit       |

**Vardiya Bilgileri**

**Terminal Market**

**Açılış Tarihi**  
03.03.2004 16:12:33

**Operatör**  
Orhan Karahasan

**Toplam Yapılan İşlem**  
11,200,000

**Tamam**

**Figure A.4.4. Market Shift Report**

In this report, again you may see the transaction information, operator and shift information. The total amount of transaction is given on the right side of the report.

### **iii. Manual Loading Center**

Pay ON-LINE system has two different loading center. One is manual loading center, and one is automated loading center. Manual loading center is operated by the accounting office of the University. Accounting office has assigned an operator to the system. This officer has the right to load the money to the cards. The interfaces of manual loading center and their explanation is given below.

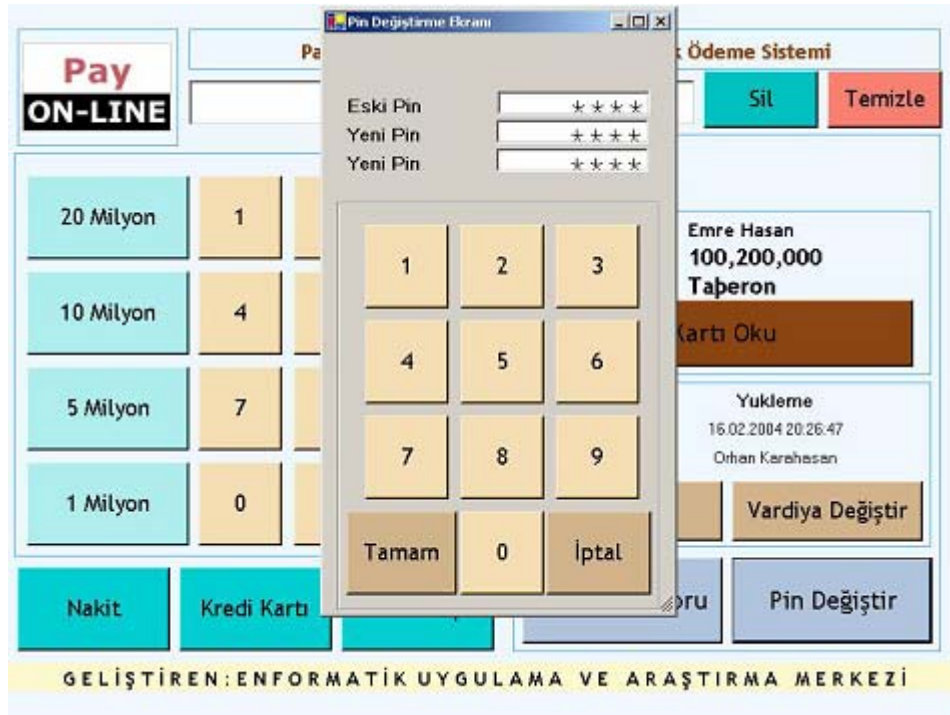
This is the entrance interface of manual loading center. In this interface, shift information, card owner information, credit card information can be seen. Each and every card has a pin inside it. The pin information is used for mistaken loading operations. Users must enter the pin of their cards to cancel the current loading transaction. You may also lock and change the shift by presenting the officer's card. This interface has special buttons on it. Those are the banknote buttons which are on

the interface to fasten the current loading transactions. You may also read the credit card information from magnetic card reader of terminal as given below interface.

Figure A.4.5. Manual Loading Center Operation Interface

Figure A.4.6. Manual Loading Center Credit Card Interface

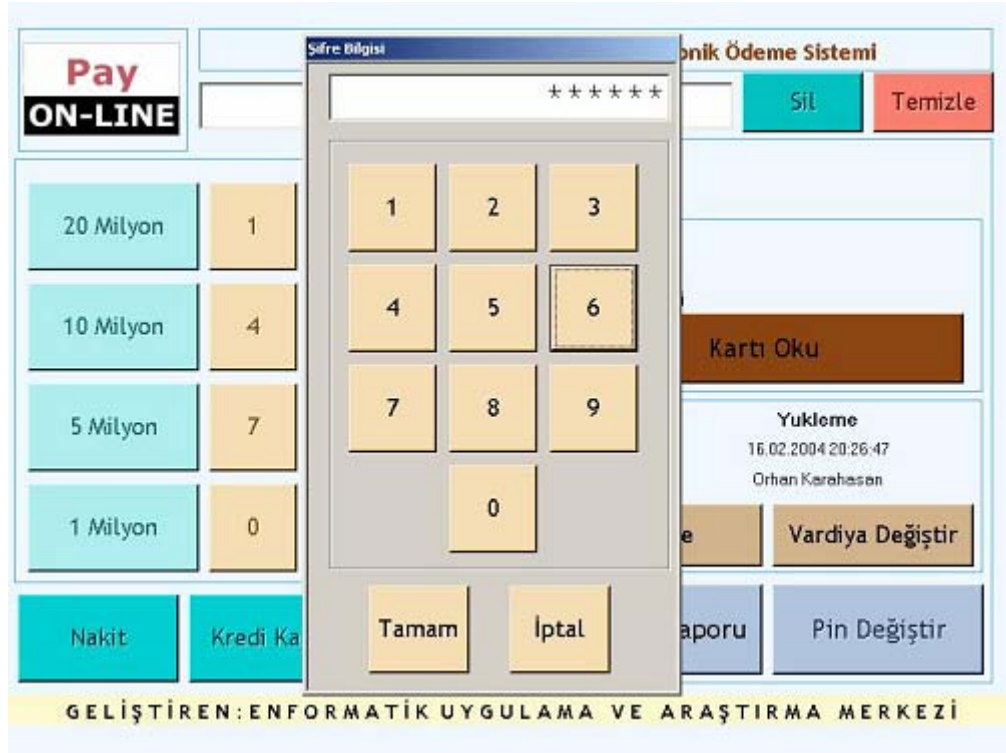
As can be seen from the screen, all credit card data is read from the card reader. But only some portion (legally defined portion) is stored in the database, because storing all credit card information is not legal.



**Figure A.4.7. Manual Loading Center PIN Interface**

To change the card's pin information, you must enter the old pin and new pin twice. Then your card pin is changed.





**Figure A.4.8. Manual Loading Center Cancel Operation Interface**

To cancel the current loading transaction, owner of the card must enter the pin of his card. This is to aware user from the situation.



**Figure A.4.9. Manual Loading Center Shift Report**

From the report section of manual loading center, you may see transaction type (credit card, cash), operator and shift information. You may also take the totals in credit card and cash dimensions from the beginning of the current shift.

*iv. Automatic Loading Center*



**Figure A.4.10. Automatic Loading Center**

Automatic Loading center works like vending machines. Users are able to load money to their cards automatically. Loading center identifies the money amount, and loads that amount to the given card. Transaction information is real time transferred to the main server. It also has the ability to work offline. In that case, the transaction information will be transferred to the server periodically.

*v. Leisure Center*

In the leisure center of the campus, there is a POS terminal defined in the payment system. This pos terminal is not so different from the market pos terminal.

**Pay ON-LINE**

Pay ON-LINE: Işık Üniversitesi Elektronik Ödeme Sistemi

Toplam 6,200,000

Tahsil Edilmiştir.

Adı Soyadı Emre Hasan  
Kalan Kredi 94,000,000  
Kullanıcı Tipi Misafir Personel

Kartı Oku

Terminal Aktivite Merkezi  
Açılış Tarihi 26.02.2004 10:10:05  
Operatör Orhan Karahasen

Kilitle Vardiya Değiştir

Tahsilat Tümü İptal Geri Al

Vardiya Raporu

GELİŞTİREN: ENFORMATİK UYGULAMA VE ARAŞTIRMA MERKEZİ

Figure A.4.11. Leisure Center Operation Interface

It can be seen from the above figure, it has a simple calculator, revenue buttons, shift buttons, and card read buttons. You may also take the current shift report using the shift report function.

**Pay ON-LINE**

Pay ON-LINE: Işık Üniversitesi Elektronik Ödeme Sistemi

Toplam

Adı Soyadı  
Kalan Kredi  
Kullanıcı Tipi

Kartı Oku

Terminal Aktivite Merkezi  
Açılış Tarihi 03.03.2004 16:12:33  
Operatör Orhan Karahasen

Kilitle Vardiya Değiştir

Tahsilat Tümü İptal Geri Al

Vardiya Raporu

GELİŞTİREN: ENFORMATİK UYGULAMA VE ARAŞTIRMA MERKEZİ

Vardiya Değiştirmek/Kapatmak için Lütfen Kartınızı Okutunuz.  
Bu Kart Sistemde Bu Operasyon için Yetkili Değildir.

Vardiya Değiştir Sistemi Kapat İptal

Figure A.4.12. Leisure Center Shift Change Interface

If you would like to change or close the current shift, and present the unauthorized card, you will get the above error. You must present the operator's card to do former operations.



**Figure A.4.13. Leisure Center Shift Report**

From the report section of leisure center module, you may take the total transaction amount, operator, shift and terminal information.

**vi. Youth Center**



**Figure A.4.14. PDA Operation Interface**

At the youth center of campus, physical network is not available. There are pocket pc's used in youth center. Shift and transaction information transferred from pocket pc to the main server periodically. During this transformation, all black list and operator information is updated at this terminal.

**vii. Vending Machines**



**Figure A.4.15. Hot Vending Machine**

There are two different types of vending machines in Pay ON-LINE. One is given above figure hot vending machines for tea-coffee, etc. The controller is attached to this hot vending machine, and data is transferred to the main server periodically.

Cold vending machines are also available to be used in Pay ON-LINE. Those vending machines are actually used to sell coke, biscuits, etc.



**Figure A.4.16. Cold Vending Machine**

Finally, Pay ON-LINE is able to work with the combi vending machines, which are for both cold and hot goods. The figure for combi automats are given below:



**Figure A.4.17. Combi Vending Machine**

***viii. Web User Terminal***

There are four different types of users of Pay ON-LINE web terminal. Those are :

- Accounting Officer
- Card Owner
- Subcontractor



**Figure A.4.18. Pay ON-LINE Web Interface**

For above type of users to enter the system, they should have username and passwords. Above figure shows the entrance page of web terminal.



**Figure A.4.19 Pay ON-LINE Accounting Officer Functions**

Above Figure shows the accounting officers function list. After the accounting officer logs into the system, he will be able to take reports on his cards depending on various dimensions, he may take various reports on the system depending on various dimensions, and he may send any bugs or errors to the administrators of the system.

After she enters the user card transaction section, he may take transaction reports daily, weekly, between two dates and monthly as given below. In this report, all loading and spending transactions are listed including the last credit amount in the card.

Pay  
ON-LINE

[Ana Sayfa](#) | [Çıkış](#)

**Pay ON-LINE > ISIKKART Kullanicisi Ana Sayfasi**

**Açıklamalar :**  
1. "Filtreler" alanından hareketlerini incelemek istediğiniz rapor tipini seçin.  
2. Seçtiğiniz rapor tipine göre istenilen tarih bilgilerini girin.  
3. Kartınızın hareketlerini görmek için "Tüketici Hareketlerini İncele" butonuna basın.

**Filtreler :**

Tüketici Hareketlerini İncele

**Tüketici Bilgileri**

|                       |            |
|-----------------------|------------|
| <b>Rapor Dönemi :</b> | 13/07/2005 |
| <b>Kart No :</b>      | 375        |
| <b>Kart Sahibi :</b>  | AZİZ GENÇ  |

**Nakit Hareketler**

|                        |   |
|------------------------|---|
| <b>Dönem Yükleme :</b> | Nakit Ödeme: 0 TL<br>K. K. Ödeme: 0 TL<br>Toplam : 0 TL |
| <b>Dönem Harcama :</b> | 0 TL  |
| <b>Dönem Toplamı :</b> | 0 TL  |

**Yemek Fisleri**

|                       |               |
|-----------------------|---------------|
| <b>Kahvaltı :</b>     | 0 TL (0 adet) |
| <b>Öde Yemeği :</b>   | 0 TL (0 adet) |
| <b>Aksam Yemeği :</b> | 0 TL (0 adet) |
| <b>Toplam :</b>       | 0 TL (0 adet) |

**Hareket Detayları**

| Terminal                                  | Tahsilat Sekli | Hareket Tipi | Tarih<br>(gg.aa.yyyy) | Tutar<br>(TL) |
|---|----------------|--------------|-----------------------|---------------|
| Girilen tarihte bir alisveris bulunamadi. |                |              |                       |               |

**Figure A.4.20. Pay ON-LINE Card Transaction Report Interface**

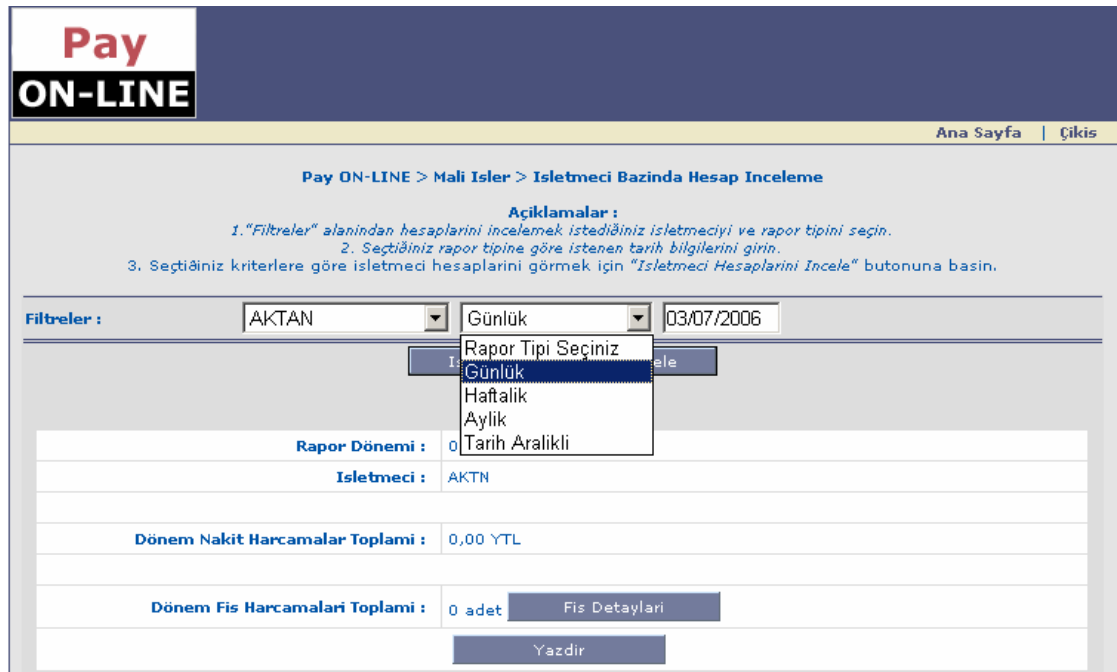
After he enters the accounting officer user's operation section, following menu appears.





**Figure A.4.21. Pay ON-LINE Accounting Officer Functions**

With the functions listed above, accounting officer users, can take various reports on subcontractor's terminals based on various criteria, and reports on manual loading center depending again on various criteria, and reports on card owner by selecting the card owner and some other criteria, and reports for automatic loading center, etc.



**Figure A.4.22. Pay ON-LINE Subcontractor Report Interface**

With the use of the first functionality of the accounting office user, he may get transaction reports depending on various criteria such as daily, weekly, monthly or between two dates. He may print the result using print button. By using the details button he may get the following report for meal scholarship information.

| Pay ON-LINE   |            |              |              |
|---|------------|--------------|--------------|
| Pay ON-LINE > Mali Isler > Isletmeci Bazinda Hesap Inceleme > Fis Detaylari |            |              |              |
| Hesap Bilgileri   |            |              |              |
| Rapor Dönemi :  | 03/07/2006 |              |              |
| Isletmeci :   | AKTN       |              |              |
|   | Kahvalti   | Öölen Yemeöi | Aksam Yemeöi |
| Toplam Burslu Öörenci:  | 0          | 0            | 0            |
| Toplam İdari Personel:  | 0          | 0            | 0            |
| Toplam Akademik Personel:   | 0          | 0            | 0            |
| Toplam Misafir Personel:  | 0          | 0            | 0            |
| Toplam Misafir:   | 0          | 0            | 0            |
| Toplam DİGER:   | 0          | 0            | 0            |
| Toplam Harcanan Fis : 0 adet  |            |              |              |

Figure A.4.23. Pay ON-LINE Meal Transaction Report

| Pay ON-LINE  |            | Ana Sayfa                            | Çıkış                 |                |
|--|------------|--------------------------------------|-----------------------|----------------|
| Pay ON-LINE > Mali Isler > Yökleme Merkezi Hesaplarını Inceleme  |            |                                      |                       |                |
| <b>Açıklamalar :</b><br>1. "Filtreler" alanından rapor tipini seçin.<br>2. Seçtiğiniz rapor tipine göre istenen tarih bilgilerini girin.<br>4. Seçtiğiniz kriterlere göre yükleme hesaplarını görmek için "Yökleme Merkezi Hesaplarını Incele" butonuna basın. |            |                                      |                       |                |
| Filtreler :  | Günlük     | 03/07/2006                           |                       |                |
| Yökleme Merkezi Hesaplarını Incele   |            |                                      |                       |                |
| Hesap Bilgileri  |            |                                      |                       |                |
| Rapor Tarihi :   | 03/07/2006 |                                      |                       |                |
| Nakit ile Yökleme Toplamı :  | 0,00       |                                      |                       |                |
| Kredi Kartı ile Yökleme Toplamı :  | 0,00       |                                      |                       |                |
| Tüm Yöklemeler Toplamı :   | 0,00       |                                      |                       |                |
| Hesap Detaylari  |            |                                      |                       |                |
| Kart No  | Operatör   | Ödeme Sekli<br>(nakit / kredi kartı) | Tarih<br>(gg.aa.yyyy) | Tutar<br>(YTL) |
| Girilen tarihte bir alisveris bulunamadi.  |            |                                      |                       |                |
| Yazdır   |            |                                      |                       |                |

Figure A.4.24 Pay ON-LINE Loading Center Report

With the second function of the accounting officer user, he may get the transaction reports on manual loading center depending on the various criteria such as daily, weekly, etc. This report is also given above.

With the third functionality of the accounting officer user, he may get the transaction reports for the card owners as given below.

Ana Sayfa | Çıkış

**Pay ON-LINE > Mali İşler > Tüketici Hareketleri İnceleme**

**Açıklamalar :**  
1. "Filtreler" alanından hareketlerini incelemek istediğiniz kart numarasını ve rapor tipini seçin.  
2. Seçtiğiniz rapor tipine göre istenilen tarih bilgilerini girin.  
3. Seçtiğiniz kartın hareketlerini görmek için "Tüketici Hareketlerini İncele" butonuna basın.

**Filtreler :** Tüm Kullanıcı Kartları | Tarih Aralıklı | 01/01/2003 | 03/07/2006  
1

**Tüketici Hareketlerini İncele**

**Tüketici Bilgileri**

|                       |                         |
|-----------------------|-------------------------|
| <b>Rapor Dönemi :</b> | 01/01/2003 - 03/07/2006 |
| <b>Kart No :</b>      | 1                       |
| <b>Kart Sahibi :</b>  | ONUR İHSAN ARSUN        |

**Nakit Hareketler**

|                  |  |
|------------------|--|
| <b>Yükleme :</b> | Nakit Ödeme:0,00 YTL<br>K. K. Ödeme: 0,00 YTL<br>Toplam : 0,00 YTL |
| <b>Harcama :</b> | 6,00 YTL   |
| <b>Toplam :</b>  | -6,000,000 YTL   |

**Yemek Fisleri**

|                       |                      |
|-----------------------|----------------------|
| <b>Kahvaltı :</b>     | 0,00 YTL (0 adet)    |
| <b>Ödle Yemeği :</b>  | 253,20 YTL (43 adet) |
| <b>Aksam Yemeği :</b> | 11,78 YTL (2 adet)   |
| <b>Toplam :</b>       | 264,98 YTL (45 adet) |

**Hareket Detayları**

**Figure A.4.25. Pay ON-LINE Card Owner Transaction Report**

With the fourth functionality of the accounting officer user, he may see the case report for automatic loading center, which shows how many banknotes from which type of banknote it contains. The report is given below.

| Pay ON-LINE   |      |
|---|------|
| Ana Sayfa   Çıkış   |      |
| Pay ON-LINE > Mali İşler > Otomatik Yükleme Kasa Raporu             |      |
| <b>Otomatik Yükleme Makinesi Kasa Raporu ( 03.07.2006 09:00:12)</b> |      |
| <b>Banknot Durumu :</b>   |      |
| 500.000   | x 0  |
| 1.000.000   | x 2  |
| 5.000.000   | x 3  |
| 10.000.000  | x 7  |
| 20.000.000  | x 18 |
| <b>Toplam : 447,00 YTL</b>  |      |
| <b>Son Bosaltılma Tarihi :</b>                                      |      |
| 22.02.2005 11:07:04   |      |
| <b>Yapılan Son Yükleme Tarihi :</b>                                 |      |
| 22.02.2005 14:21:10   |      |

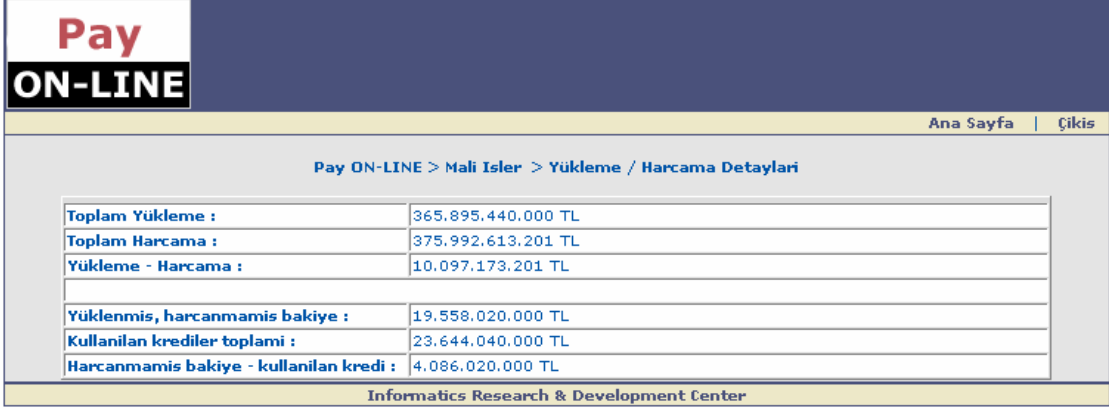
**Figure A.4.26. Pay ON-LINE Automatic Loading Center Report**

In the general reporting section, he may get reports in various dimensions as can be seen in the following figure.

| Pay ON-LINE  |   |           |                |            |                 |            |                 |                |                |                |                |            |            |               |                  |                       |                   |           |             |                 |   |
|--|---|-----------|----------------|------------|-----------------|------------|-----------------|----------------|----------------|----------------|----------------|------------|------------|---------------|------------------|-----------------------|-------------------|-----------|-------------|-----------------|---|
| Ana Sayfa   Çıkış  |   |           |                |            |                 |            |                 |                |                |                |                |            |            |               |                  |                       |                   |           |             |                 |   |
| Pay ON-LINE > Mali İşler > Genel Sorgulama Ekranı  |   |           |                |            |                 |            |                 |                |                |                |                |            |            |               |                  |                       |                   |           |             |                 |   |
| <b>Açıklamalar :</b>   |   |           |                |            |                 |            |                 |                |                |                |                |            |            |               |                  |                       |                   |           |             |                 |   |
| 1. "Filtreler" alanından hesaplarını incelemek istediğiniz işletmeyi ve rapor tipini seçin.                |   |           |                |            |                 |            |                 |                |                |                |                |            |            |               |                  |                       |                   |           |             |                 |   |
| 2. Seçtiğiniz rapor tipine göre istenen tarih bilgilerini girin.   |   |           |                |            |                 |            |                 |                |                |                |                |            |            |               |                  |                       |                   |           |             |                 |   |
| 3. Raporu değişik sıralamak için "Sıralama" alanlarını değiştirin.   |   |           |                |            |                 |            |                 |                |                |                |                |            |            |               |                  |                       |                   |           |             |                 |   |
| 4. Seçtiğiniz kriterlere göre işletme hesaplarını görmek için "İşletme Hesaplarını İncele" butonuna basın. |   |           |                |            |                 |            |                 |                |                |                |                |            |            |               |                  |                       |                   |           |             |                 |   |
| <b>Filtreler :</b>   | <table border="1"> <tr> <td>İşletme :</td> <td>Tüm İşletmeler</td> </tr> <tr> <td>Operatör :</td> <td>Tüm Operatörler</td> </tr> <tr> <td>Terminal :</td> <td>Tüm Terminaller</td> </tr> <tr> <td>Hareket Tipi :</td> <td>Tüm Hareketler</td> </tr> <tr> <td>Harcama Tipi :</td> <td>Tüm Harcamalar</td> </tr> <tr> <td>Fis Tipi :</td> <td>Tüm Fisler</td> </tr> <tr> <td>Kart Sahibi :</td> <td>Tüm Kullanıcılar</td> </tr> <tr> <td>Kullanıcı Departman :</td> <td>Tüm Departmanlar:</td> </tr> <tr> <td>Kart No :</td> <td>Tüm Kartlar</td> </tr> <tr> <td>Tarih Aralığı :</td> <td>Tarih 1 <input type="text"/> Tarih 2 <input type="text"/></td> </tr> </table> | İşletme : | Tüm İşletmeler | Operatör : | Tüm Operatörler | Terminal : | Tüm Terminaller | Hareket Tipi : | Tüm Hareketler | Harcama Tipi : | Tüm Harcamalar | Fis Tipi : | Tüm Fisler | Kart Sahibi : | Tüm Kullanıcılar | Kullanıcı Departman : | Tüm Departmanlar: | Kart No : | Tüm Kartlar | Tarih Aralığı : | Tarih 1 <input type="text"/> Tarih 2 <input type="text"/> |
| İşletme :  | Tüm İşletmeler  |           |                |            |                 |            |                 |                |                |                |                |            |            |               |                  |                       |                   |           |             |                 |   |
| Operatör :   | Tüm Operatörler   |           |                |            |                 |            |                 |                |                |                |                |            |            |               |                  |                       |                   |           |             |                 |   |
| Terminal :   | Tüm Terminaller   |           |                |            |                 |            |                 |                |                |                |                |            |            |               |                  |                       |                   |           |             |                 |   |
| Hareket Tipi :   | Tüm Hareketler  |           |                |            |                 |            |                 |                |                |                |                |            |            |               |                  |                       |                   |           |             |                 |   |
| Harcama Tipi :   | Tüm Harcamalar  |           |                |            |                 |            |                 |                |                |                |                |            |            |               |                  |                       |                   |           |             |                 |   |
| Fis Tipi :   | Tüm Fisler  |           |                |            |                 |            |                 |                |                |                |                |            |            |               |                  |                       |                   |           |             |                 |   |
| Kart Sahibi :  | Tüm Kullanıcılar  |           |                |            |                 |            |                 |                |                |                |                |            |            |               |                  |                       |                   |           |             |                 |   |
| Kullanıcı Departman :  | Tüm Departmanlar:   |           |                |            |                 |            |                 |                |                |                |                |            |            |               |                  |                       |                   |           |             |                 |   |
| Kart No :  | Tüm Kartlar   |           |                |            |                 |            |                 |                |                |                |                |            |            |               |                  |                       |                   |           |             |                 |   |
| Tarih Aralığı :  | Tarih 1 <input type="text"/> Tarih 2 <input type="text"/>   |           |                |            |                 |            |                 |                |                |                |                |            |            |               |                  |                       |                   |           |             |                 |   |
| <b>Sorgula</b>   |   |           |                |            |                 |            |                 |                |                |                |                |            |            |               |                  |                       |                   |           |             |                 |   |

**Figure A.4.27. Pay ON-LINE General Report Interface**

With the last functionality of accounting user, spending/loading report may be taken from the system as given below.




The screenshot shows the 'Pay ON-LINE' interface. The header includes the logo 'Pay ON-LINE' and navigation links 'Ana Sayfa' and 'Çıkış'. The main content area displays a table with financial data under the heading 'Pay ON-LINE > Mali İşler > Yükleme / Harcama Detayları'. The table lists various financial metrics and their corresponding values in TL. At the bottom, it identifies the 'Informatics Research & Development Center'.

| Pay ON-LINE > Mali İşler > Yükleme / Harcama Detayları |                    |
|--|--------------------|
| Toplam Yükleme :                                       | 365.895.440.000 TL |
| Toplam Harcama :                                       | 375.992.613.201 TL |
| Yükleme - Harcama :                                    | 10.097.173.201 TL  |
| Yüklenmiş, harcanmamış bakiye :                        | 19.558.020.000 TL  |
| Kullanılan krediler toplamı :                          | 23.644.040.000 TL  |
| Harcanmamış bakiye - kullanılan kredi :                | 4.086.020.000 TL   |

Informatics Research & Development Center

**Figure A.4.28. Pay ON-LINE total spending/loading report**

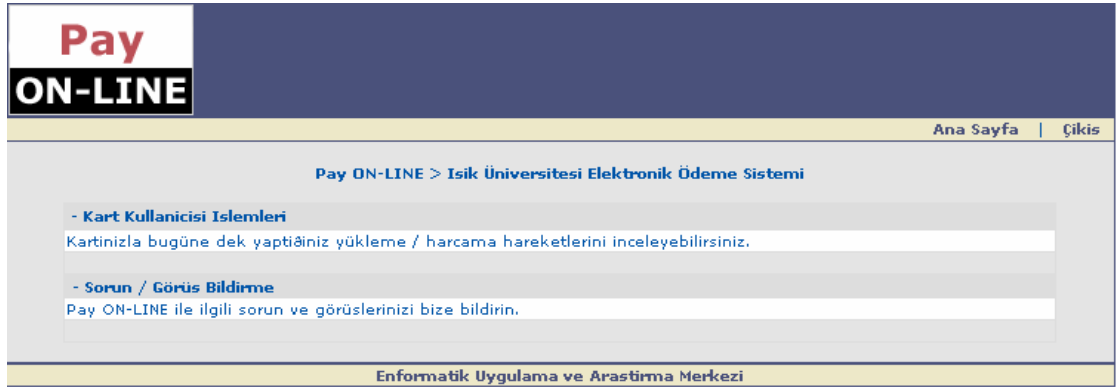
With the last functionality of the current user, he may send any problems related to the system to the system administrators as given below.



The screenshot shows the 'Pay ON-LINE' feedback interface. The header includes the logo 'Pay ON-LINE' and navigation links 'Ana Sayfa' and 'Çıkış'. The main content area displays the title 'Pay ON-LINE > ISIKKART Kullanıcısı Sorun / Öneri Bildirme' and the user's name 'Kullanıcı Adı: AZİZ GENÇ' and card number 'Kart No: 375'. Below this, there is a section titled 'Sorun / Öneri Bildirme' with a prompt: 'Pay ON-LINE ile ilgili sorun ve görüşlerinizi bize bildirin.' There are two input fields: 'Başlık:' and 'Mesaj:'. A 'Gönder' button is located at the bottom right of the form.

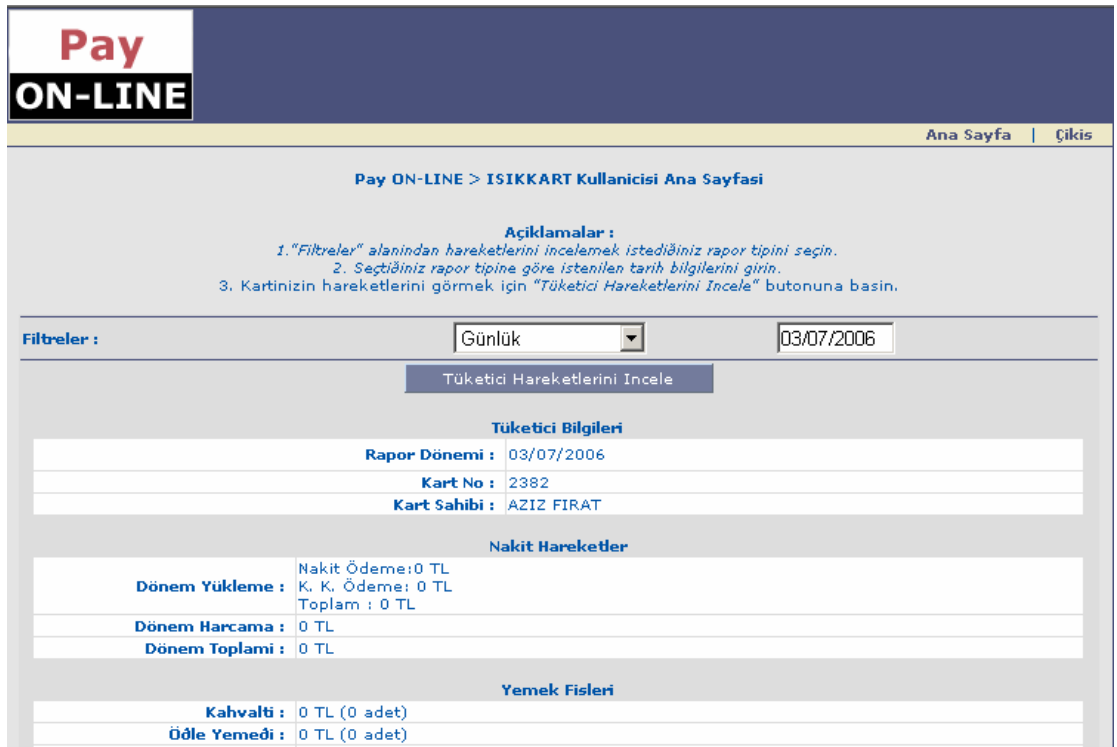
**Figure A.4.29. Pay ON-LINE Feedback Interface**

The following figure shows the menu of the card owner. With the use of this menu, he may get the reports on his card transactions and also send any problems to the system administrator.



**Figure A.4.30. Pay ON-LINE Card Owner Functions**

Reporting section of the card owner is given below. He may get reports on various diminutions for his card payment transactions.



**Figure A.4.31. Pay ON-LINE Card Owner Report Interface**

He may also send any problems related to the system to the owners of the system using the following interface.

**Figure A.4.32. Pay ON-LINE Feedback Interface**

Subcontractors may take any type of reports for their registered terminals using the following report tool.

**Figure A.4.33. Pay ON-LINE Subcontractor Report Interface**

He may also send any problems related to the system to the system administrator using the following interface.

**Pay**  
**ON-LINE**

Ana Sayfa | Çıkış

Pay ON-LINE > ISIKKART Kullanicisi Sorun / Öneri Bildirme

Kullanici Adi: Hakan Kavaklioglu

Kart No:

**Sorun / Öneri Bildirme**  
Pay ON-LINE ile ilgili sorun ve görüşlerinizi bize bildirin.

Baslik:

Mesaj:

Gönder

**Figure A.4.34. Pay ON-LINE Feedback Interface**



## **A.5. Pay ON-LINE Modules**

There are six different modules that will be explained in this section.

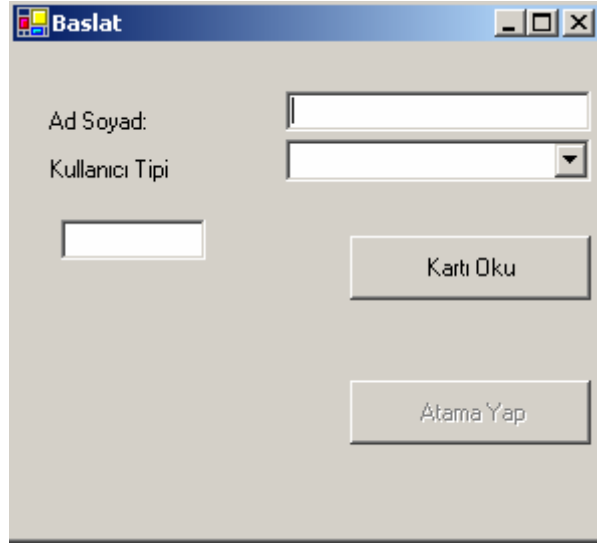
- Reporting Module
- Card Initialization Module
- Money Loading Module
- Information Retrieval & Update Module
- Terminal Monitoring Module
- Data Transfer Module
- Credit Spending Module
- Card Information Update Module

### ***i. Reporting Module***

This module is integrated with the reporting sections of web user interfaces and also terminal's shift report sections. Those sections are explained deeply in former sections, so they are not again explained.

### ***ii. Card Initialization Module***

Pay ON-LINE cards are printed in card printers. After press operation, cards are initialized or personalized. In this process, card owner information is passed to the card and user types, credit amounts are initialized. Card initialization module interface is given below.



**Figure A.5.1. Card Initialization Interface**

As can be seen from the above figure, user type, name & surname information and number of meal scholarship is entered to the system. It opens an account for the current user, and initializes the user card with the given information.

**iii. Money Loading Module**

This module is explained deeply in former sections. It is not again explained. It is used for loading the credit amount to the cards.

**iv. Information Retrieval & Update Module**

This module is used for updating the black list,etc information at the terminals and take the transaction information from the terminals. This module is integrated with the POS terminals.

**v. Terminal Monitoring Module**

This module is used for real time monitoring of Pay ON-LINE terminals. Interface of this module is geiven below.

| Pay ON-LINE Terminals |                       |            |                       |
|-----------------------|-----------------------|------------|-----------------------|
| Terminal ID           | Terminal Name         | Ip Number  | Status                |
| 1                     | Leisure Center        | 10.150.2.2 | down                  |
| 2                     | Market                | 10150.2.1  | Un expected Shut down |
| 3                     | Dining Hall           | 10.150.2.3 | up                    |
| 4                     | Manual Loading Center | 10.150.2.4 | down                  |

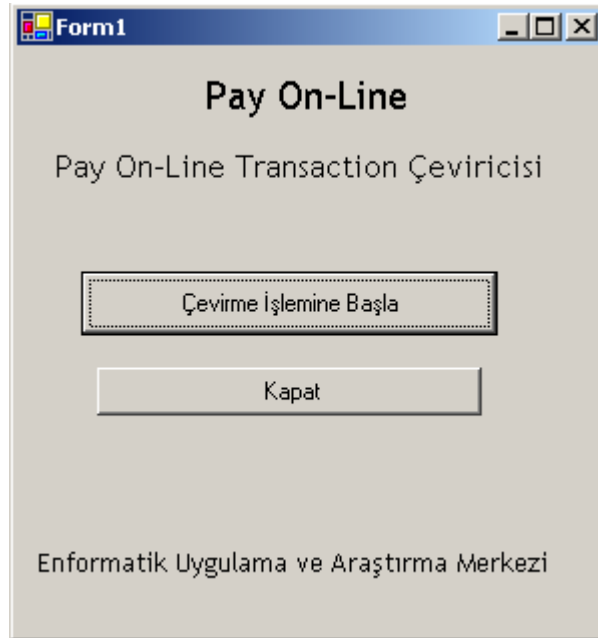
**Figure A.5.2. Terminal Monitoring Software Interface**

**vi. Card Information Update Module**

This module is used for updating the current card information. If the card is in black list, it is blocked, if there is any job in the card job list, that operation is done on the card automatically. This module is integrated on every pos terminal.

**vii. Data Transfer Module**

This module is used for offline terminals to transfer data after collection by use of pocket PC's. Pocket PC is connected to pc through USB interface. By using this module, it reads the transaction information from the pocket pc and sends it to the server. The user interface of this module is given below.



**Figure A.5.3. Data Transfer Module Interface**

***viii. Credit Spending Module***

This module is used for spending credits on the cards. This module is integrated to all POS terminals. It works as a basket. You may cancel the current transaction fro all elements in the basket or individually for the elements of a basket.

## **A.6 Pay ON-LINE Users**

There are five different users defined in Pay ON-LINE system. Those are

- Card owners
- Accounting Officer
- Operator
- Manager
- Subcontractor

### ***Card Owners***

Each card is owned by a user at the campus. With the use of this card, they may spend their credit in the card or load credit to their card. They may take various reports on their spendings and loads operations on their cards depending on some dimensions.

### ***Accounting Officer***

Accounting officer is a user who takes reports on credit loads and spendings on various dimensions, and report the result and do payments of the subcontractor's transaction amounts periodically.

### ***Operator***

Operator is the user who operates the POS terminals at each terminal. Their cards are defined as an operator to the system and their cards must be read at the pos terminals to begin a shift.

### ***Manager***

If the problem occurs, or the operator forgets to close or change the shift, manager is able to close his shift. In other words, they are able to close the locked and opened shifts by using their manager cards.

## ***Subcontractor***

Subcontractors may also take reports on various dimensions for their POS terminal defined in the system using web interfaces. Using their reports, they may claim their payments from the system for the given criterias.