FACULTY OF FUNDAMENTAL PROBLEMS OF TECHNOLOGY
WROCŁAW UNIVERSITY OF TECHNOLOGY

PRESCRIPTION MANAGEMENT SYSTEM
THE PATIENT MODULE

Z. DOBOSIEWICZ & M. NIEMCZYK
P. NUŻKA & B. PACIOREK & B. PIWOWARSKI

WROCŁAW 2014

Contents

1 CURRENT SITUATION

The main element of the currently used system is a paper prescription. It contains all information required to buy specific medicines, e.g.:

- prescription's creation date
- patient's personal data:
  - name and surname
  - address
  - PESEL
- number of the prescription, specific for each doctor
- list of medicines with level of refund, signature and stamp of the doctor

The patient, who was given the prescription by the doctor, goes to the pharmacy to buy the medicines. He gives his prescription to a pharmacist and says which of the medicines from the list he wants to buy. The pharmacist checks if the medicines are available and if yes, he sells them. Next, he takes the prescription and makes a signature next to the each of the medicine he sold. He also inputs to the software installed on computers in the pharmacy, which of the medicine was sold, for who, who gave the prescription and what are the costs of the refund.

A report, including detailed information about each prescription sold in the pharmacy, is generated each month. This report is sent to the NFZ central database. NFZ refunds the costs of the medicines based on this report. Each prescription has to be kept in the pharmacy for at least five years, and should be ready for controls made by NFZ representatives.

2 PATIENT'S MODULE

2.1 MODULE DESCRIPTION

The prescription system from the patient point of view is based on smart cards. Each patient has a unique card with ID and a pair of cryptographic keys used to create a signature. The system could be easily combined with electronic IDs, when they become available in Poland.

The benefit of our system is that the patient could get the prescription without leaving home. He could request medicines by calling the doctor, who would prescribe them and make available on patient's account. In order to decrease the refund fraud problem, the patient has to realize the prescription in pharmacy by himself. If he is unable to realize it, he would be able to transfer it onto another person's account. Realization of a transferred prescription would only be possible for the person designed by the patient. However, if the patient would like to change the designed person or make the prescription again available for him to realize, he would be able to cancel the transfer.

Both the patient and the doctor (with patient's permission) are able to browse all of the patient's previous prescriptions. It could be helpful to reduce possibility of interactions between drugs prescribed by different specialists. Also, doctors would not be able to abuse this functionality, because it would require the patient to insert his smart card into the terminal in doctor's office.

Patient is able to browse the list of medicines, doctors and pharmacies. Thanks to this, he could easily check the leaflet of the medicine, find the phone number to the doctor or check the opening hours of the pharmacy.

2.2 GOALS OF THE PATIENT MODULE

- Protection from the refund fraud problem
- Possibility to get prescriptions without leaving home
- Functionality of transferring prescription to another person's account
- Availability of prescription history for a doctor

- Possibility to browse the list of medicines, doctors and pharmacies

3 THREATS AND INCONVENIENCES

The way prescriptions are currently processed is vulnerable to many threats, and brings many inconveniences. The most important ones are listed below.

Party	**Threats and Inconveniences**
patient	• the patient can lose the prescription and he cannot buy the medicines, even if they are lifesaving, he has to go to the doctor again and ask for the new prescription • the patient can lose his prescription, then, the person who found this prescription can buy this medicines; what is more, this person can get to know, who takes which medicines and in this way, he can get to know, what is wrong with the person described on the prescription
NFZ	• significant amount of money is being defrauded from NZF, because the current system does not verify if the patient himself has bought the medicine or the pharmacists has made a false call for the medicine having some patient's prescription, prepared by the doctor (who is also a part of the defraudation scheme)
system	• the patient can try to copy the prescription and try to buy the medicines few times in different pharmacies • the patient can claim that he has lost his prescription and ask the doctor to give him another one, then, he can buy the medicines twice instead of once

3.1 PROTECTION METHODS

3.1.1 SMART CARD

The main reason we decided to use smart cards is that smart card solutions, which employ two factor authentication, i.e. "something you have and something you know", provide a high security level which is crucial for the prescription system sensitive data.

All of the system's users will be given personalized smart cards which will store their identification data: names, surnames, PESEL and digital certificates. Each card would have PIN number associated with it, that will be used to initialize authentication process.

To improve the security level of the system, the data stored on smart cards should be encrypted. Users' private keys need to be stored in a secure memory which cannot be directly read out.

In case of loosing a smart card, the user should perform a standardized revocation procedure, i.e. he should block a card in the assigned institution. The user should enroll for a new card afterwards

3.1.2 CERTIFICATES

Each user has his digital certificate on his smart card. All of the user's certificates must be given by a defined certification authority and regularly updated.

The certificate's validity should be checked at each use of the user's smart card. The validity check is performed in the database module.

4 SYSTEM ARCHITECTURE

The patient's module architecture consists of the following elements:

- smart card with personal certificate and secure key storage, used for the authentication and signing
- patient's application, providing all of the functionalities required by patient's module:
  - provides user-friendly interface
  - is connected with patient's card and the database
  - establishes two way SSL connection
- database is a central element of the whole system; stores the data and handles all the necessary database I/O functions; the database is described in greater detail in Database & Server Documentation'

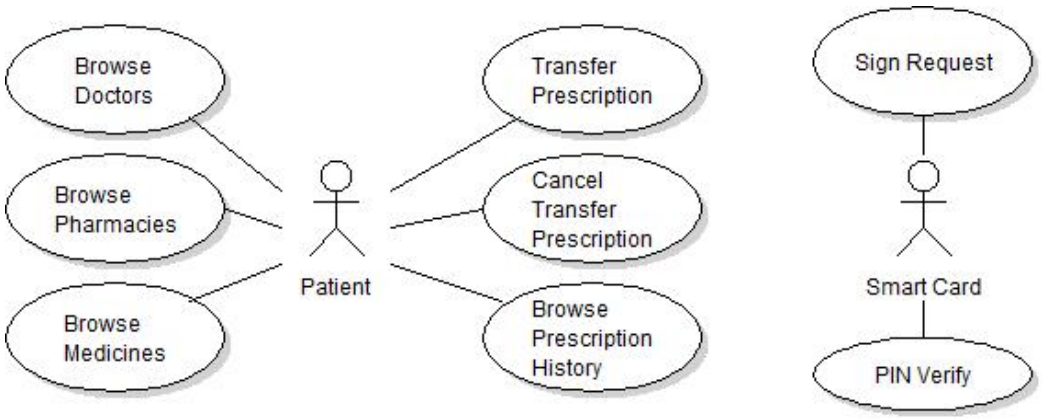

Figure 1: Use cases

5 USE CASES

Patients have access to the system by dedicated patient's application. Each patient is given unique, personal smart card that is being used for authentication.

5.1 USE CASES FOR PATIENT'S APPLICATION

The patient's application is a graphical interface to the patient's module. It includes six use cases that are available for the patient:

browse medicines
: The patient is able to browse all medicines available in the database. There is a leaflet attached to each medicine's description, that contains at least dosage and contraindications.

browse pharmacies
: The patient is able to browse all pharmacies available in the database. Each pharmacy has its address and opening hours listed for patient's convenience.

browse doctors
: The patient is able to browse all doctors available in the database. He can

find phone number and office address for each doctor.

browse prescription history
The patient can browse all of his prescriptions, differentiated on active and already realized.

transfer prescription
If the patient cannot realize prescription, he is able to transfer his prescription buying rights to somebody else.

cancel prescription transfer
The patient can cancel transfer of prescription and realize it by himself or transfer it again.

5.2 SMART CARD USE CASES

The smart card, introduced into the system for security reasons, includes two use cases.

sign message
The smart card signs a message produced by patient's application. The signature would be used in calls to database procedures.

verify PIN
The smart card verifies PIN, that the patient has entered, in order to access any functionalities of the system.

5.3 FLOW CHART FOR TRANSFER PRESCRIPTION USE CASE

To transfer the prescription user has to enter correct PIN. Application establish connection with database and retrieve the list of prescription available to transfer. The list contains only prescriptions which can be transferred by the patient. Then the patient is able to select prescription to transfer from the list and enter the new owner's ID. After the patient's confirm transfer, application create and send request to the database. If the signature under the request concatenated with nonce is valid and request contains required data database transfers the prescription to the new owner.

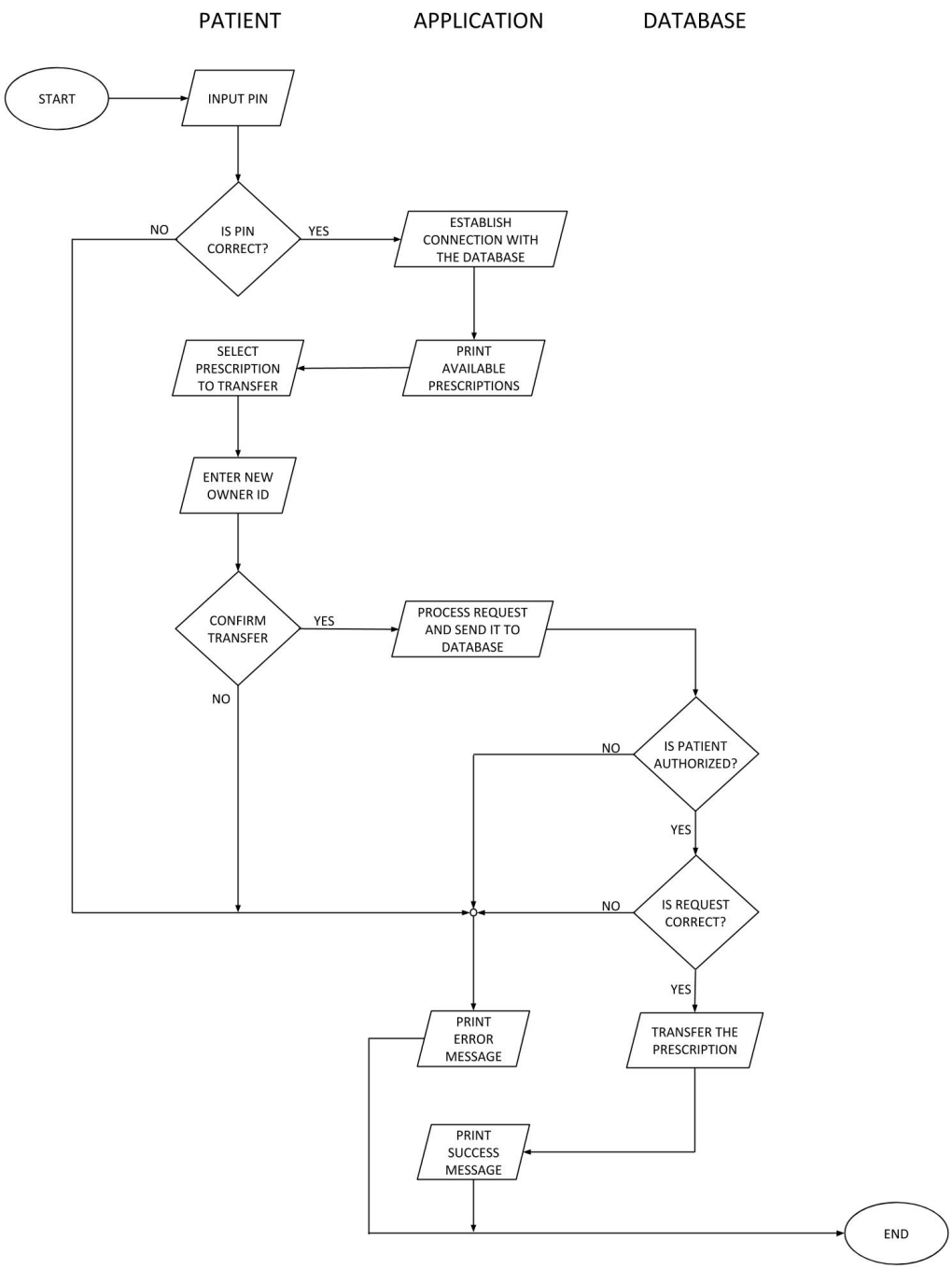

Figure 2: Transfer prescription flow chart

6 FUNCTIONALITIES OF APPLICATION

The application implements following functions:

- `browse_medicines`
- `browse_pharmacies`
- `browse_doctors`
- `browse_prescription_history`
- `transfer_prescription`
- `cancel_prescription_transfer`

They are discussed in greater detail below.

6.1 BROWSE MEDICINES

	`browse_medicines`
argumets	• `name` • `type`
description	The patient is able to browse all medicines available in database.
action	After entering name of medicine, function is querying database for results.
display	• `name` • `prescription requirement` • `patient information leaflet`

6.2 BROWSE PHARMACIES

	`browse_pharmacies`
argumets	• `name` • `address`
description	The patient is able to browse all pharmacies available in database.
action	After entering name or address of pharmacy, function is querying database for results.
display	• `name` • `address` • `phone` • `opening hours`

6.3 BROWSE DOCTORS

	`browse_doctors`
argumets	• `name` • `address` • `license number`
description	The patient is able to browse all doctors available in database.
action	After entering name of doctor or address, function is querying database for results.

display	• `name` • `address` • `phone`

6.4 BROWSE PRESCRIPTION HISTORY

	`browse_prescription_history`
argumets	• `time interval` • `isExecuted`
description	The patient is able to browse all of his previous prescriptions.
action	Function is querying database for results, using patient's ID and signature created by the smart card.

display	• medicine name • quantity • unit • dosage • execution • time of execution • doctor name • doctor signature • pharmacist name • pharmacy signature

6.5 TRANSFER PRESCRIPTION

	transfer_prescription
argumets	• new owner ID • prescription ID
description	The patient can transfer the prescription to another person.
action	After entering ID of designed person and choosing the prescription, function that transfers it is called, using patient's ID and signature created by the smart card.

display	• `new owner ID` • `exit status`

6.6 CANCEL PRESCRIPTION TRANSFER

	`cancel_prescription_transfer`
argumets	• `prescription ID`
description	The patient is able to transfer his prescription back into his account.
action	After choosing the prescription, function that rolls back the transfer is called, using patient's ID and signature created by the smart card.
display	• `exit status`

7 FUNCTIONALITES OF PATIENT'S CARD

The patient's card implements following functions:

- `sign`
- `PIN verify`

They are discussed in greater detail below.

7.1 SIGN REQUEST

	`sign`
argumets	• `message`
description	The patient's card signs doctor or pharmacist request.
action	The patient's card makes a signature under doctor or pharmacist message using its secret key.
result	• `signature` • `exit status`

7.2 PIN VERIFICATION

	`PIN_verify`
argumets	• `PIN`
description	The card verifies the PIN given by patient.
action	The patient's card verifies correctness of the PIN entered by the patient.

result	• `exit status`

8 SEQUENCE DIAGRAMS

8.1 SEQUENCE DIAGRAM FOR CONNECTION INITIALIZATION

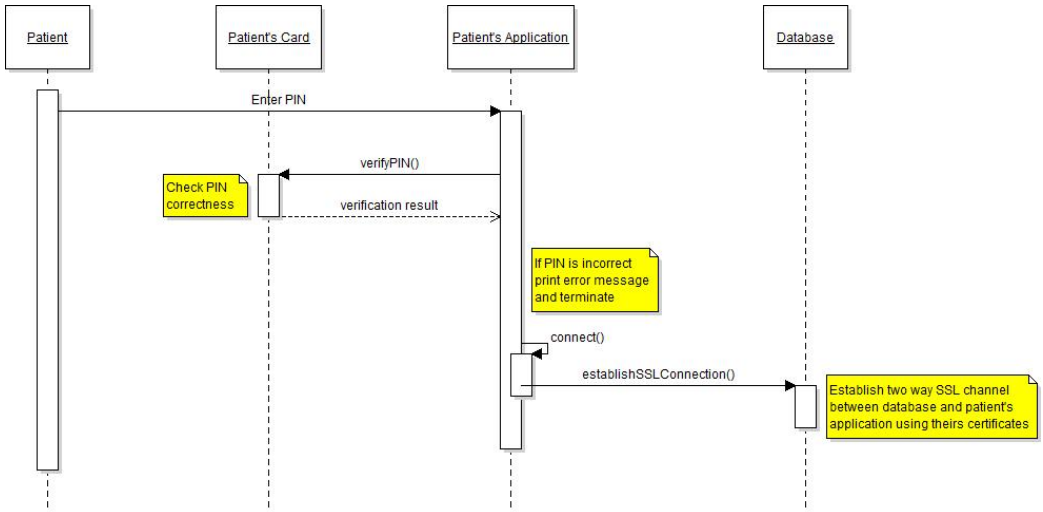

Figure 3: Connection initialization

When the patient connects to the system, he needs to enter the PIN. Then, the PIN is verified by the Patient's Card. If the verification fails, an error message is printed and the connection is terminated. Otherwise, the Patient's Application establishes a two-way SSL channel with the database. From this point, the communication between the Patient's Application and the database is done through SSL encrypted channel.

8.2 SEQUENCE DIAGRAM FOR TRANSFER PRESCRIPTION FUNCTIONALITY

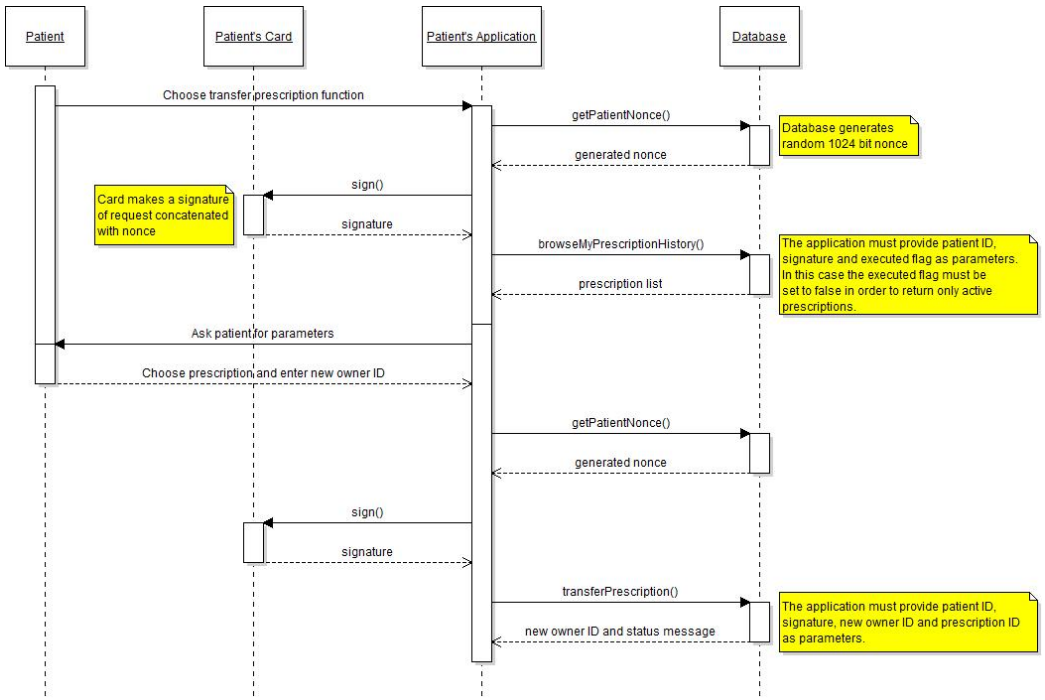

Figure 4: Transfer prescription

This sequence is executed after establishing a secure connection with the database.

To transfer a prescription, the patient has to choose transfer prescription functionality in the Patient's Application (PA). PA sends patient's ID to the database and receives a random 1024 bit nonce. Afterwards, PA sends created browse prescriptions request to the Patient's Card (PC) for signing. PA sends the signed request to the database (DB) and receives a list of available prescriptions. Then the patient chooses a prescription he wants to transfer from the list, and enters new owner's ID. Next, PA requests new nonce from DB and creates a valid transfer prescription request, which is signed by PC. The request with a signature is sent to DB afterwards. DB verifies both the request and the signature. If the verification was successful, DB transfers the prescription to the new owner and returns a status message and the ID of new owner.

8.3 SEQUENCE DIAGRAM FOR BROWSE MEDICINES FUNCTIONALITY

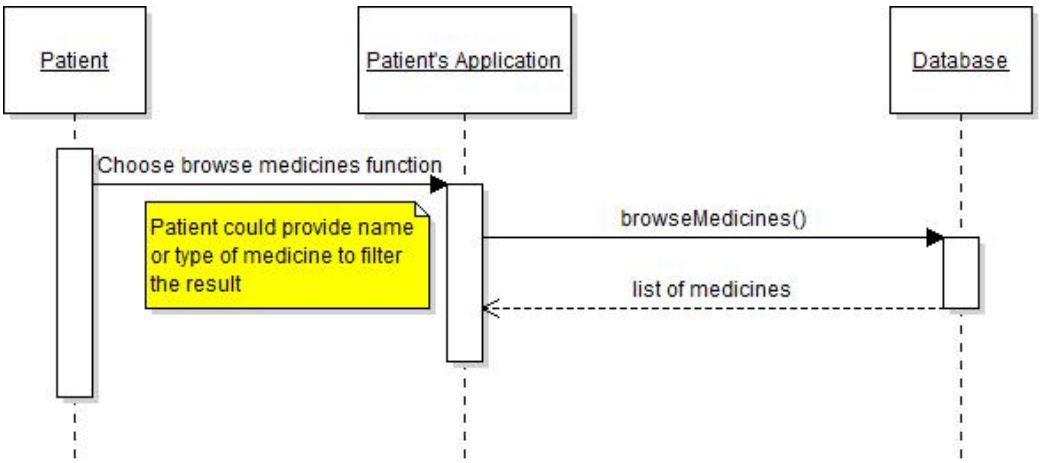

Figure 5: Browse medicines

To browse medicines, the patient needs to choose browse medicines functionality in the Patient's Application. Then, the Patient's Application prepares a request with parameters either default or provided by the patient. The request is sent to the database afterwards. The database returns a list of medicines which is displayed to the patient in the Patient's Application.

9 SECURITY

Both security mechanisms used in the patient's module and their justification are described in the following sections.

9.1 USED SECURITY MECHANISMS

9.1.1 SMART CARD

Entity	Description
Patient's card	Patient's card stores private key along with the certificate. Elements of the certificate are as follows (text in parentheses describes what is used): • Serial Number: Used to uniquely identify the certificate • Subject: The person, or entity identified (personal data of the patient). • Signature Algorithm: The algorithm used to create the signature (RSA). • Signature: The actual signature to verify that it came from the issuer. • Issuer: The entity that verified the information and issued the certificate (CA for the patient). • Valid-From: The date the certificate is first valid from. • Valid-To: The expiration date. • Public Key: The public key. • Thumbprint Algorithm: The algorithm used to hash the public key certificate (SHA256). • Thumbprint (also known as fingerprint): The hash itself, used as an abbreviated form of the public key certificate.

Card's data access	• Card is read only is the sense that patients are not able to modify the data that is stored on it. They do, however (after successful authentication), have access to certificate stored on the card as well as the function to sign arbitrary input data with its private key.
PIN	• The certificate access/signing input data can be performed after entering PIN. The user is given 4-digit PIN and the verification system will allow three attempts before blocking the card.

9.1.2 AUTHENTICATION

Patient's authentication is constructed as a two factor process. It includes the following points:

- Something you have - smart card (containing user's certificate)
- Something you know - PIN needed to access smart card's functionalities

9.1.3 CONNECTION

The connection between the application and the database is established by two-way SSL protocol. Whole communication afterwards would be sent by encrypted SSL channel. We assume that if the connection was lost, the whole authentication process needs to be repeated.

9.2 JUSTIFICATION

9.2.1 PIN PROTECTION

The PIN number is used to authenticate the cardholder. We propose 4-digit PIN number. Three subsequent incorrect attempts will block the card. Similar mechanism is already used e.g. in ATM cards.

9.2.2 SECURE COMMUNICATION WITH THE DATABASE

The communication channel between the database and the application is secured with a two way SSL protocol. We assume that SSL provides all necessary mechanisms to protect the channel from attacks.

9.2.3 PROTECTION AGAINST PRESCRIPTION OVERTAKING

Transfer prescription request have to be signed by the patient using his private key in order to not give buying rights to unauthorized person. If the patient has made a mistake during prescription transfer, he is able to cancel and redo the transfer correctly.

9.2.4 PROTECTION AGAINST PRESCRIPTION DUPLICATION

Transfer and cancel transfer prescription functionalities have to be performed in transaction environment by the database. In this way, there would be no possibility that both the patient and new owner could buy the prescription simultaneously.

9.3 Advantages of system

Our system is designed in way that any defraudation of purchasing not prescribed medicine is impossible, pharmacist can not do any defraudation on transaction of seeling drugs to the patient which were not previously prescribed by the doctor, because to every transaction our system demands patient's smart card with previously issued prescription by the doctor and signed by his smart card.

The above security assure very secure system of digital signatures and certificates which will be implemented in our application on smart cards and users programs. This system will prevent any defraudation from users (patient/ pharmacist/ doctor) and also simplify any financial settlement between pharmacist and NFZ, furthermore system will be very comfortable and easy to use for every user.