

# Prescriptions Management



WROCLAW, 2014

# Authors

## Database Group

Michał KACZMAREK

Paweł KĘDZIA

Jakub PŁASKONKA

Mateusz PŁATEK

## Patient Group

Zbigniew DOBOSIEWICZ

Maciej NIEMCZYK

Paweł NUŻKA

Bartłomiej PACIOREK

Bartosz PIWOWARSKI

## Doctor Group

Krystian KRAKOWIAK

Piotr LIPIAK

## Pharmacy Group

Olga DZIĘGIELEWSKA

Marcin KLEPACZKA

Andrzej RYBCZAK

Jan SZAJDA

## PROJECT MANAGER

Olga DZIĘGIELEWSKA

## SUPERVISOR

Ph.D. Łukasz KRZYWIECKI

# Contents

<b>I</b>	<b>INTRODUCTION</b>	<b>8</b>
<b>1</b>	<b>CURRENT SITUATION</b>	<b>9</b>
<b>2</b>	<b>THREATS AND INCONVENIENCES</b>	<b>11</b>
2.1	NFZ . . . . .	11
2.1.1	DEFRAUDATION . . . . .	11
2.2	PATIENT . . . . .	12
2.2.1	LOSING A PRESCRIPTION . . . . .	12
2.2.2	INTERNET SHOPPING . . . . .	12
2.3	PHARMACY . . . . .	12
2.3.1	REFUNDATION DELAY . . . . .	12
2.3.2	PRESCRIPTIONS WITH MISTAKES . . . . .	12
2.4	SYSTEM . . . . .	12
2.4.1	PRESCRIPTION FORGERY . . . . .	12
2.4.2	PRETENDING THAT PRESCRIPTION WAS LOST . . . . .	13
<b>3</b>	<b>SYSTEM GOALS</b>	<b>14</b>

3.1	CENTRAL SERVER OBJECTIVES . . . . .	15
3.2	PHARMACY MODULE OBJECTIVES . . . . .	15
3.3	PATIENT MODULE OBJECTIVES . . . . .	16
<b>II</b>	<b>PROJECT</b>	<b>17</b>
<b>1</b>	<b>PROJECT</b>	<b>18</b>
1.1	ENVIRONMENT REQUIREMENTS . . . . .	18
1.1.1	SMART CARDS . . . . .	18
1.1.2	TWO-WAY SSL . . . . .	19
1.1.3	CERTIFICATES . . . . .	19
1.1.4	PHARMACY . . . . .	20
1.2	ARCHITECTURE . . . . .	20
1.2.1	CENTRAL SERVER ARCHITECTURE . . . . .	20
1.2.2	USERS MODULES . . . . .	20
1.3	PROTECTION AND SECURITY . . . . .	21
1.3.1	PROTECTION METHODS . . . . .	21
1.3.2	JUSTIFICATION . . . . .	23
<b>III</b>	<b>DATABASE</b>	<b>25</b>
<b>1</b>	<b>USE CASES</b>	<b>26</b>
1.1	Shared use cases . . . . .	27

1.2	PATIENT . . . . .	28
1.3	DOCTOR . . . . .	29
1.4	PHARMACIST . . . . .	29
1.5	SPECIAL USERS . . . . .	30
<b>2</b>	<b>COMMUNICATION</b>	<b>32</b>
2.1	CONNECTING TO CENTRAL SERVER . . . . .	32
2.2	NONCES & VERIFICATION PROCESS . . . . .	34
<b>3</b>	<b>DATABASE FUNCTIONS AND SCHEMA</b>	<b>36</b>
3.1	DATABASE FUNCTIONS . . . . .	36
3.1.1	SHARED FUNCTIONS . . . . .	36
3.1.2	PATIENT FUNCTIONS . . . . .	38
3.1.3	DOCTOR FUNCTIONS . . . . .	41
3.1.4	PHARMACIST FUNCTIONS . . . . .	43
3.2	DATABASE SCHEMA . . . . .	46
<b>4</b>	<b>CENTRAL SERVER SECURITY STANDARDS</b>	<b>47</b>
4.1	PHYSICAL SECURITY . . . . .	47
4.2	DATA ENCRYPTION . . . . .	48
4.3	BACKUP PROCEDURE . . . . .	48

<b>IV</b>	<b>PHARMACY MODULE</b>	<b>49</b>
<b>1</b>	<b>DATA FLOWS</b>	<b>50</b>
1.1	USE CASES . . . . .	50
1.2	SCENARIO . . . . .	52
<b>2</b>	<b>SEQUENCE DIAGRAM</b>	<b>54</b>
2.1	COMMUNICATION INITIALIZATION . . . . .	54
2.2	ESTABLISH A SECURE COMMUNICATION . . . . .	56
2.3	SELECT PRESCRIPTION TO BUY . . . . .	56
2.4	REALIZE PRESCRIPTION . . . . .	56
2.5	END OF THE PROTOCOL . . . . .	57
<b>V</b>	<b>PATIENT MODULE</b>	<b>59</b>
<b>1</b>	<b>DATA FLOWS</b>	<b>60</b>
1.1	USE CASES . . . . .	60
1.2	SMART CARD USE CASES . . . . .	61
1.3	SCENARIO: PRESCRIPTIONS TRANSFER . . . . .	62
<b>2</b>	<b>FUNCTIONALITES OF THE PATIENT'S CARD</b>	<b>64</b>
2.1	SIGN REQUEST . . . . .	64
2.2	PIN VERIFICATION . . . . .	65
<b>3</b>	<b>SEQUENCE DIAGRAMS</b>	<b>66</b>

3.1	SEQUENCE DIAGRAM FOR CONNECTION INITIALIZATION . . . . .	66
3.2	SEQUENCE DIAGRAM FOR TRANSFER PRESCRIPTION FUNCTIONALITY . .	67
3.3	SEQUENCE DIAGRAM FOR BROWSE MEDICINES FUNCTIONALITY . . . . .	68
<b>VI</b>	<b>DOCTOR MODULE</b>	<b>69</b>
<b>1</b>	<b>DATA FLOWS</b>	<b>70</b>
1.1	USE CASES . . . . .	70
1.2	ACTIVITY DIAGRAM . . . . .	71
<b>2</b>	<b>SEQUENCE DIAGRAM</b>	<b>72</b>
2.1	VIEW ENTIRE PATIENT'S HISTORY . . . . .	73
2.2	NOTES . . . . .	74
<b>3</b>	<b>PRESCRIPTION</b>	<b>75</b>
<b>4</b>	<b>SIGNATURES</b>	<b>77</b>
4.1	DOCTOR SIGNATURE OVER PRESCRIPTION, AND PHARMACIST SIGNATURE AS A PROOF THAT PRESCRIPTION IS REALIZED . . . . .	77
4.2	PATIENT NEEDS TO GENERATE SIGNATURE WHEN PATIENT ARCHIVAL PRESCRIPTION HAS TO BE AVAILABLE . . . . .	78

## Part I

# INTRODUCTION



# Chapter 1

## CURRENT SITUATION

Current system strongly depends on paper prescriptions. Each prescriptions carries a lot of data, which some can be treated as private data of patients:

- prescription's creation date,
- patient's personal data:
  - name and surname
  - address
  - PESEL
- number of the prescription, specific for each doctor <sup>1</sup>,
- list of medicines with refoundation level,
- 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

---

<sup>1</sup>NFZ generates a list of prescription for each doctor. Every prescription has the unique identifier number. During the refoundation process, NFZ checks, if the number on the prescription, the doctor name, signature and stamp are correct. Only if they are valid, the refoundation is granted.

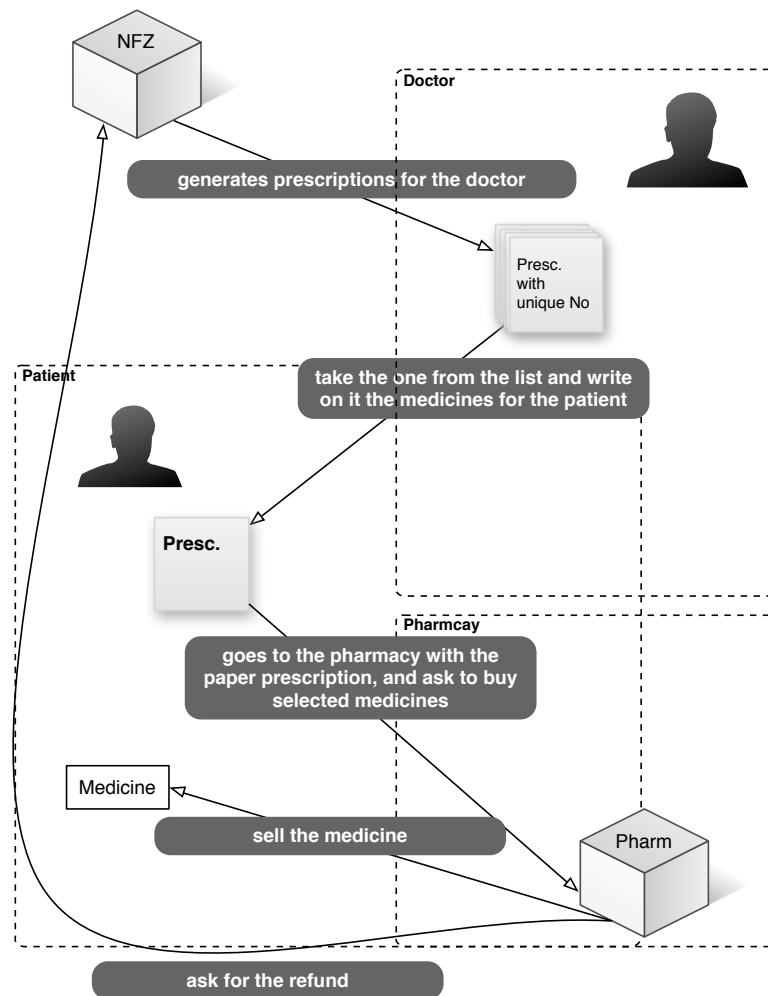


Figure 1.1: The main points of currently used system

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 refundation costs.

Each month in every pharmacy a report, consisting of the set of the information about each prescription sold in the pharmacy is generated. This report is sent to the NFZ central database. Based on this, the NFZ refunds costs of the medicines. Each prescription has to be kept for at least five years in the pharmacy, and be ready for checking during controls made by NFZ representatives.

## Chapter 2

# 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.

### 2.1 NFZ

#### 2.1.1 DEFRAUDATION

Significant amount of money is being defrauded from NFZ 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). Example situation: Let say that we have 2 corrupted parties in the current system - a doctor and a pharmacist. In that situation the doctor can create a fake prescription for any of his patient, then send it to the pharmacist and he - as a second party - can declare that the prescription, which is financed by NFZ, as completed.



## **2.2 PATIENT**

### **2.2.1 LOSING A PRESCRIPTION**

The patient can lose the prescription and he cannot buy the medicines, even if they are life-saving, he has to go to the doctor again and ask for the new prescription.

### **2.2.2 INTERNET SHOPPING**

Today we can only buy in an online pharmacy medicines which can be bought without a prescription.

## **2.3 PHARMACY**

### **2.3.1 REFUNDATION DELAY**

The pharmacy has to wait long time to refund costs for the medicines from NFZ.

### **2.3.2 PRESCRIPTIONS WITH MISTAKES**

Prescription tend to contain mistakes which makes it useless. In this situation the patient has to go to the doctor again so it's fixed.

## **2.4 SYSTEM**

### **2.4.1 PRESCRIPTION FORGERY**

Patient can try to copy the prescription and try to buy the medicines few times in different pharmacies.



### **2.4.2    PRETENDING THAT PRESCRIPTION WAS LOST**

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.

## Chapter 3

# SYSTEM GOALS

The main objectives of our new design of the prescription management system is to limit the impact of the threats listed in Chapter 2 and improve the usability of the current system. It will meet each of following requirements:

1. Prescriptions will be digitalized.
2. Prescriptions will be hard to forge.
3. Doctors will not be able to create prescriptions without knowledge of patient.
4. Prescriptions will be realized only by users with right credentials.
5. Patients and doctors will be able to browse history of prescriptions.
6. System will be secured with most up-to-date measures.
7. System will provide anonymous big data statistics.

### **3.1 CENTRAL SERVER OBJECTIVES**

The central server will be the core component of the whole digital prescriptions system. Key features of the central server are:

- storing data of patients, doctors and pharmacists,
- allowing doctors to create prescriptions,
- allowing doctors and patients to review history of created prescriptions,
- allowing patients to transfer the ownership of prescription in secure, controllable manner,
- allowing pharmacists to review prescriptions yet to be realized,
- allowing prescription realization only if patient will be present at this event,
- validating the signatures of each party,
- providing anonymous statistics.

### **3.2 PHARMACY MODULE OBJECTIVES**

The pharmacy module objectives are:

- The patient has to be sure that his sensitive data is stored in a secure way, and unauthorized person cannot get to know anything about his medicines and illnesses.
- The pharmacist has to be sure that he sells the right medicines only for the right patient.
- The refund process should be quicker and easier.
- The possibility of making mistakes on the prescription should be eliminated.
- The number of defraudations should be significantly limited.

### 3.3 PATIENT MODULE OBJECTIVES

The patient's module objectives are:

- 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.

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.



## Part II

# PROJECT

# Chapter 1

## PROJECT

### 1.1 ENVIRONMENT REQUIREMENTS

#### 1.1.1 SMART CARDS

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

All the system's users will be given personalized smart cards which will store their identification data: names, surnames, PESEL and digital certificates. Each card will be assigned PIN and PUK numbers. The first one will be used to initialize authentication process, the second one will be used for unblocking a card<sup>1</sup>.

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

Keys used for connecting and authorizing should have sufficient length to provide security. If the RSA key is used it should have length of at least 2048 bits.

---

<sup>1</sup>Unblocking procedure can be performed in the two following situation: when a user inputs wrong PIN number three times in a row or when he blocks his card after losing it.

In case of loosing a smart card, a user should perform a standardized revocation procedure. First, he should block a card in the assigned institution and while doing this he should be able to select whether he want to block the card temporarily or permanently. In the first case, after finding the card it is possible to unblock it with card's PUK number. In the second case it is necessary to generate new user's card and even after finding the card it will not be possible to unblock it.

### 1.1.2 Two-WAY SSL

Two-Way SSL provides the same functionalities as SSL, with the addition of authentication and non-repudiation of the client authentication, using digital signatures. When mutual authentication is used the server would request the client to provide a certificate in addition to the server certificate issued to the client. The main advantages of client-certificate authentication are:

1. The private information (the private key) is never sent to the server. The client doesn't let its secret out at all during the authentication.
2. A server that doesn't know a user with that certificate can still authenticate that user, provided it trusts the CA (Certificate Authority) that issued the certificate (and that the certificate is valid). This is very similar to the way passports are used: you may have never met a person showing you a passport, but because you trust the issuing authority, you're able to link the identity to the person.

### 1.1.3 CERTIFICATES

In Two-Way SSL both parties (client and server) need the certificates. Each user has his digital certificate on his smart card. All the user's certificates must be given by a defined certification authority and regularly<sup>2</sup> updated. The CA also generates a keypair for the database server.

In case of selecting permanent blocking option during the revocation procedure, a new certificate is generated for such user.

---

<sup>2</sup>The CA should define a standard validity period for the patient's, pharmacist's and doctor's certificates.

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.

#### **1.1.4 PHARMACY**

All the pharmacies which will be using the system must have broadband internet access, two smart card readers and two terminals: one for a pharmacist and one for a customer. The terminals apart from displaying the data need to handle all the confirmation actions on both sides.

### **1.2 ARCHITECTURE**

#### **1.2.1 CENTRAL SERVER ARCHITECTURE**

Central server will be constructed of several components. In order to provide all necessary data and functionalities to the users this system will be a cooperation of system's logic, specific APIs and database. In the project the following components were chosen:

1. **server layer** - Apache HTTP Server ("Apache") version 2.4.9
2. **database layer** - PostgreSQL version 9.3

#### **1.2.2 USERS MODULES**

The users modules architecture consists of the following elements:

1. **smart cards** with personal certificate, used for the authentication and signing, and an application which allows to read certain data from the card;
2. **pharmacist's PC, patient's PC or doctor's PC** with a corresponding module application which provides all of the functionalities which satisfy all the operation

- performed by the pharmacists, doctor or a patient; provides two user-friendly interfaces; is connected with appropriate terminals and the central database; is able to execute SIGMA protocol, handle secure keys storage and establish SSL connection;
3. **central DB** is a central element of the whole system; stores the data and handles all the necessary database I/O functions.

## 1.3 PROTECTION AND SECURITY

Below we describe entities used in the system, how we choose to protect them and why.

### 1.3.1 PROTECTION METHODS

#### 1.3.1.1 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.

#### 1.3.1.2 PHARMACIST'S CARD

Pharmacist's card stores the same information as patient's card, with exception to several certificate fields being different:

- **Subject:** *Personal data of the pharmacist and pharmacy*
- **Issuer:** *CA for the pharmacies*

#### 1.3.1.3 CARD'S DATA ACCESS

Card is read only in the sense that patients/pharmacists 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.

#### 1.3.1.4 PIN

The certificate access/signing input data can be performed after inputting a PIN. The user is given 4-digit PIN number and the verification system will allow three attempts of typing the correct number before the card is blocked.

#### 1.3.1.5 PATIENT AUTHENTICATION

Two factor authentication is used:

- Something you have - smart card (containing user's certificate)
- Something you know - PIN number used to access the certificate on the card

#### 1.3.1.6 PHARMACIST AUTHENTICATION

Two factor authentication is used:

- Something you have - smart card (containing pharmacist's certificate)
- Something you know - PIN number used to access the certificate on the card

#### **1.3.1.7 CONNECTION BETWEEN CARD AND APPLICATION**

After successful authentication we establish a session key and the communication is encrypted with it. For that AKE protocol „SIGMA” is utilized. (Note that encryption is optional if we assume that no eavesdropping can take place or the data exchanged isn't considered confidential).

#### **1.3.1.8 CONNECTION BETWEEN APPLICATION AND CENTRAL DATABASE**

Two-way SSL connection is used along with additional nonce-based authentication.

### **1.3.2 JUSTIFICATION**

#### **1.3.2.1 PIN PROTECTION**

The PIN number is used to authenticate the card holder. In case the card was lost and found by someone else, he won't be able to use the card without knowing the PIN. We propose 4-digit PIN number with three subsequent incorrect attempts before the card is blocked as it's already used e.g. in ATM cards and proven to work there.

#### **1.3.2.2 SIGMA PROTOCOL**

This AKE protocol (we choose to use SIGMA, but that is by no means the ultimate choice. It's been chosen due to convenience of having the implementation already in place. If one wishes, it can be replaced by other AKE protocol, e.g. NAXOS, NAXOS+, SMQV, CMQV, UKS, KCI, eKCI) will be used to secure the communication channels between parties existing in the pharmacy, i.e. cards and application. AKE protocols provide not only secure communication but also authentication mechanism, preventing

not only eavesdropping or man-in-the-middle attacks but also assures security under ephemeral and static keys leakage.

#### **1.3.2.3 SECURE KEY DISPOSAL**

All short term keys, i.e. ephemeral keys used using AKE protocol or session keys which are the result of the protocol are erased from memory immediately after they are no longer needed.

#### **1.3.2.4 SECURE COMMUNICATION WITH THE DATABASE**

The communication channel between database and pharmacy is secured with an SSL connection. We assume the SSL provides all the necessary mechanisms to protect the channel from attacks. To strengthen the security of the channel all the requests from any valid party must contain the signature (RSA signature) over the nonce provided by database system. This solution ensure that no unauthorized party is able to get access to database.

#### **1.3.2.5 PROTECTION AGAINST DEFRAUDATION**

Each transaction has to be signed by all the participating parties. In this setting it is impossible for the doctor/pharmacist to fake the medicaments sale and deceive NFZ into giving them money for refunding the nonexistent costs, as signature of the patient is also required. Additionally a token that has to be signed changes with each transaction, so protection from repetition attacks is also gained.



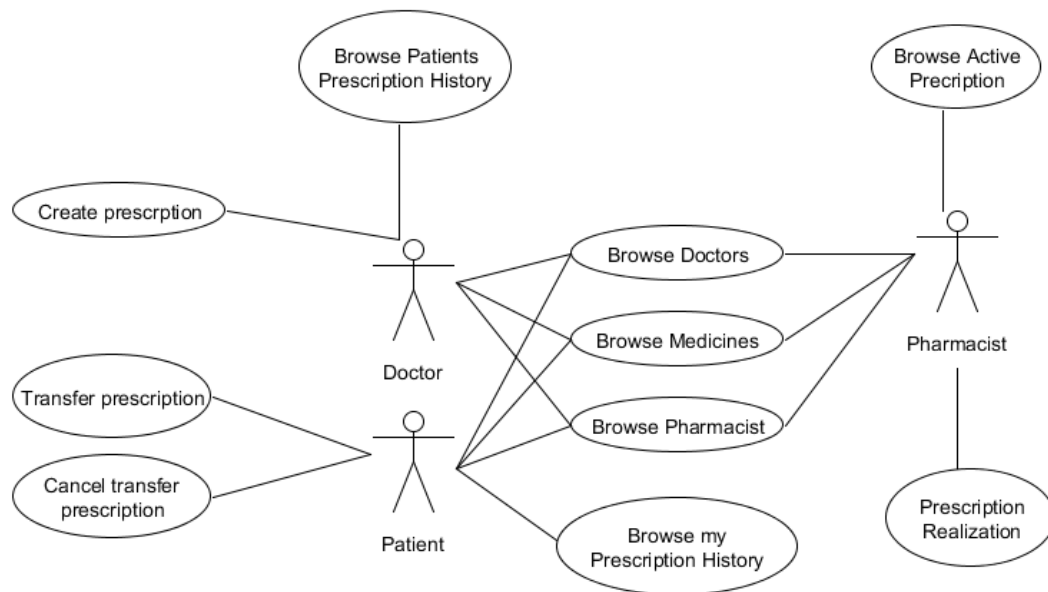
## Part III

# DATABASE

# Chapter 1

## USE CASES

We define two groups of actors - clients like patients, doctors and pharmacists which benefit from the system on daily basis and third parties - administrators, analytic tools and government authorities which cope with the system on special occasions.



Every use case requires the users to establish secure channel of communication with central server and have to be logged in which will be described more thoroughly in section 2.1.

## 1.1 Shared use cases

Three use cases are applicable for patient, pharmacist and doctors and they consider browsing informations which can be publicly accessible, that is:

- Browse Doctors
- Browse Medicines
- Browse Pharmacists

Rest of use cases which are applicable to only one actor is described in their respective subsections.

Actors: Patient, Doctor, Pharmacist	Title: Browse Doctors
Goal:	Allows to find doctor with specific name, address or license number.
Scenario:	User enters any or all of name, address and license number of searched doctor.
Result:	List of doctors corresponding to the query.
Database method:	<b>browse_doctors</b>

Actors: Patient, Doctor, Pharmacist	Title: Browse Pharmacies
Goal:	Allows to find pharmacist and pharmacy with specific name, address or license number.
Scenario:	User enters any or all of name, address, license number of searched pharmacist or pharmacy name.
Result:	List of pharmacists corresponding to the query.
Database method:	<b>browse_pharmacies</b>

Actors: Patient, Doctor, Pharmacist	Title: Browse Medicines
Goal:	Allows to find medicine with specific name or type.
Scenario:	User enters name or/and type of medicine he is searching.
Result:	List of medicines corresponding to the query.
Database method:	<b>browse_medicines</b>

## 1.2 PATIENT

Actors: Patient	Title: Transfer prescription
Goal:	Allows to transfer a prescription to another patient and give him credentials to realize this prescription. Patient who transferred the prescription losses his right to realize it by himself. If he wants the prescription back he has to cancel the transfer (next use case).
Scenario:	Patient enters his id, id of new owner, the prescription id he wants to transfer and his signature.
Result:	OK response from database and iId of new owner of prescription.
Database method:	<b>transfer_prescription</b>

Actors: Patient	Title: Cancel Transfer Prescription
Goal:	Allows to revert transferring of prescription to another patient.
Scenario:	Patient enters his id, prescription id he wants transfers to revert and his signature.
Result:	OK response from database.
Database method:	<b>cancel_prescription_transfer</b>

Actors: Patient	Title: Browse My Prescriptions History
Goal:	Patient can see his history of realized and created prescriptions.
Scenario:	Patient sends his id which is signed by his key from smartcard. Patient can define the time span of returned prescriptions as also a filter to only return prescriptions which aren't realized yet.
Result:	List of prescriptions for the patient.
Database method:	<b>browse_prescription_history</b>

### 1.3 DOCTOR

Actors: Doctor	Title: Create prescription
Goal:	Allows to create a new prescription in database for selected patient..
Scenario:	Doctor enters his and patients ids, as well as the data specific to the medicine - id, dosage, unit and quantity. Everything is signed by his key.
Result:	OK response from database.
Database method:	<code>create_prescription</code>

Actors: Doctor	Title: Browse Patients Prescriptions History
Goal:	Doctor can see patient history of realized and created prescriptions..
Scenario:	Doctor sends his id - he will see all prescriptions created by him. If he will add the id of patient with patients signature, he will see the full history of prescriptions of current patient. Doctor can define the time span of returned prescriptions as also a filter to only return prescriptions which aren't realized yet.
Result:	List of prescriptions for the patient.
Database method:	<code>browse_patient_prescription_history</code>

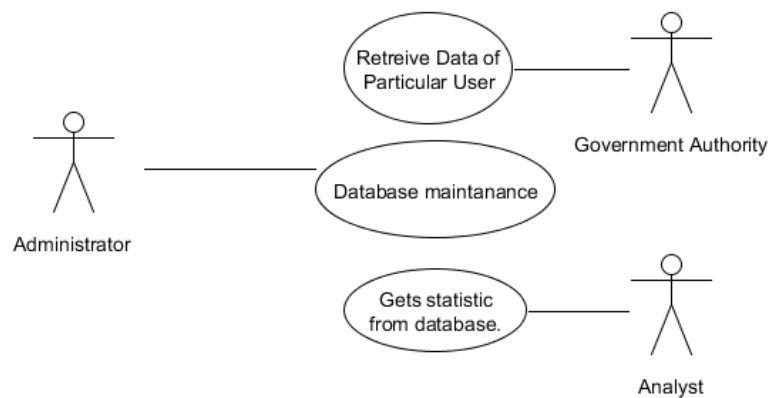
### 1.4 PHARMACIST

Actors: Pharmacist	Title: Prescription realization
Goal:	Pharmacist realizes the prescription. DB checks if the request can be verified and if the prescription is valid.
Scenario:	Pharmacist enters his id, prescription id as well as drugs id, dosage and quantity of medicine. Everything is signed by pharmacist key.
Result:	OK response from database if operation was successful.
Database method:	<code>prescription_realization</code>

Actors: Pharmacist	Title: Browse Active Prescriptions
Goal:	Pharmacist can see prescriptions which are not yet realized.
Scenario:	Pharmacist sends his id and id of current patient which are signed by both of their keys. Pharmacist can see only prescriptions which are not yet realized.
Result:	List of prescriptions for the patient.
Database method:	<code>browse_active_prescriptions</code>

## 1.5 SPECIAL USERS

There are also defined three other users which cope with the system on special occasions. These are - administrator, which maintains the system, analytic tools which can be used to obtain statistical data and the government authority which has super access to all the data after acquiring proper permissions from court or police.



Actor: Administrator	Title: Central Server maintenance
Goal:	Administrator modifies the database, upgrades software etc.

Actor: Government Authority	Title: Retrieve Data Of Particular User
Goal:	Government Authority (GA) can retrieve all sensitive data of every user after showing permission to do so e.g. court order. GA account password can be separated into several pieces to ensure that one attacker won't be in possession of the key.

Actor: Analytic tools	Title: Obtaining statistics from DB
Goal:	Analyst can query the database for statistical data e.g. number of medicines sold in last month. Analyst can't query patients or link prescriptions data to particular person.

## Chapter 2

# COMMUNICATION

Every communication with database can be described by one abstract scenario. First central server and client establish session via SSL. After correct establishment of session, client chooses one of database functions that he can execute with appropriate arguments. Before using methods requiring signatures, client has to ask server for nonce, generated specially for the user. After obtaining the nonce, client can execute selected function. Database verifies the correctness of signature and data passed in arguments and returns the result, or if one of the verification steps failed, error message.

### 2.1 CONNECTING TO CENTRAL SERVER

1. Enter smartcard with users private key and certificate (or establish paths to them)
2. set path of PostgreSQL to environment variable PATH.
3. in command line write

```
psql 'host=hosts_ip port=port_address dbname=database_name
user=username sslmode=require sslcert=user.crt sslkey=user.key
sslrootcert=ca.crt'
```

where:

- **host** - IP of server where database is



- `dbname` - is the name of database to which we want to connect
- `user` - name of user which want to connect. Each part will have its own user name.
- `sslcert` - certificate of user.
- `sslkey` - private key of user.
- `sslrootcert` - Certificate of CA.

Example login:

```
psql 'host=95.85.28.156 port=5432 dbname=PrescriptionSystemMk2
user=patient sslmode=require sslcert=patient.crt sslkey=patient.key
sslrootcert=ca.crt'
```

4. enter password

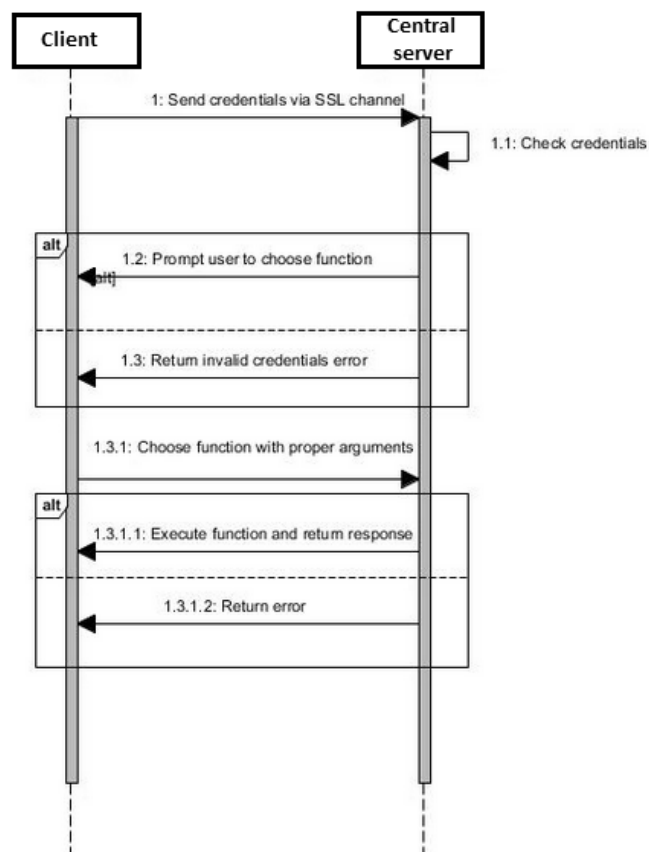


Figure 2.1: General communication diagram for patient, pharmacist and doctor

## 2.2 NONCES & VERIFICATION PROCCES

Randomly generated nonces are part of challenge-response protocol used in communication with database layer. Nonce are security measure against the replay attack. If a request require signature of any party, client has to ask database for generated nonce for given ID. After nonce is return, client has to:

1. Conacatenate function name,
2. function arguments,
3. nonce.
4. Calculate SHA-1 sum over the concatenated elements.
5. Sign the with appropriate key<sup>1</sup>.
6. Add the signature as the corresponding argument in function.
7. Send the request.

When the server obtains the request:

1. Takes users key from the database
2. Validates the signature
3. If the signature is validated, constructs SHA-1 sum in the same way as user
4. compares the verified, signed sum with one calculated in previous point
5. Executes the query if the sums are equal
6. Returns the result to the user

---

<sup>1</sup>Signing method should be equal to invoking openssl command "openssl rsautl sign" with necessary parameters only

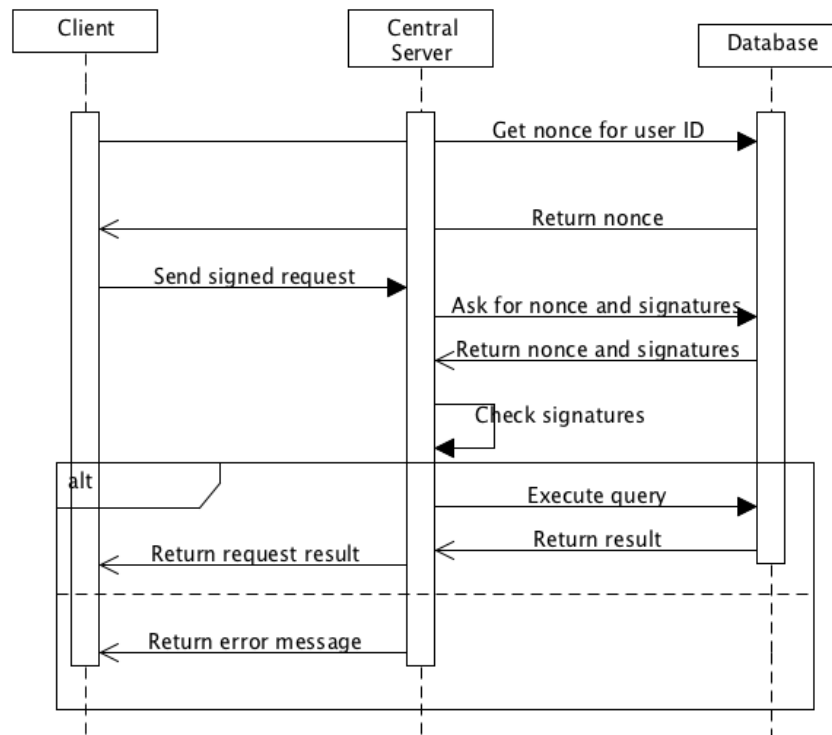


Figure 2.2: Sequence diagram of executing request with nonce signature

## Chapter 3

# DATABASE FUNCTIONS AND SCHEMA

### 3.1 DATABASE FUNCTIONS

After verifying credentials sent by user to Central Server via SSL secure channel, user, depending on its role, will be able to execute set of functions, which will serve single purpose each (e.g. creation of new prescription).

#### 3.1.1 SHARED FUNCTIONS

	<code>browse_medicines</code>
Arguments:	<ul style="list-style-type: none"><li>• <code>name</code> (string, optional, default = None)</li><li>• <code>type</code> (string, optional, default = None)</li></ul>
Usage:	Pharmacist sends his id and id of current patient which are signed by both of their keys. Pharmacist can see only prescriptions which are not yet realized.

Result:	<ul style="list-style-type: none"><li>• <code>medicine_id</code></li><li>• <code>name</code></li><li>• <code>prescription requirement</code></li><li>• <code>medicine type</code></li><li>• <code>maximum dosage</code></li><li>• <code>unit</code></li></ul>
---------	---

Note: Multiple records may be returned at single request.

	<code>browse_doctors</code>
Arguments:	<ul style="list-style-type: none"><li>• <code>name ( string, optional, default = None)</code></li><li>• <code>address (string, optional, default = None)</code></li><li>• <code>license_number (string, optional, default = None)</code></li></ul>
Usage:	Entity using this function performs simple query which return all public data regarding registered doctors stored in DB. Arguments name, adress and license_number narrows down result applying filters to the executed query.
Result:	<ul style="list-style-type: none"><li>• <code>doctor_id</code></li><li>• <code>name</code></li><li>• <code>address</code></li><li>• <code>license_number</code></li><li>• <code>certificate</code></li><li>• <code>public_key</code></li></ul>

Note: Multiple records may be returned at single request.

	<code>browse_pharmacists</code>
Arguments:	<ul style="list-style-type: none"> <li>• <code>pharmacist_name</code> ( string, optional, default = None)</li> <li>• <code>address</code> (string, optional, default = None)</li> <li>• <code>license_number</code> (string, optional, default = None)</li> <li>• <code>pharmacy_name</code> (string, optional, default = None)</li> </ul>
Usage:	Entity using this function performs simple query which return all public data regarding registered pharmacists stored in DB. Arguments name, adress and license _number narrows down result applying filters to the executed query.
Result:	<ul style="list-style-type: none"> <li>• <code>pharmacist_id</code></li> <li>• <code>name</code></li> <li>• <code>address</code></li> <li>• <code>license_number</code></li> <li>• <code>certificate</code></li> <li>• <code>public_key</code></li> <li>• <code>pharmacy_name</code></li> </ul>

Note: Multiple records may be returned at single request.

### 3.1.2 PATIENT FUNCTIONS

	<code>get_patient_nonce</code>
Arguments:	<ul style="list-style-type: none"> <li>• <code>patient_id</code> (integer, mandatory)</li> </ul>
Usage:	Function returns 1024 bit nonce for given patient _id.
Result:	<ul style="list-style-type: none"> <li>• <code>nonce</code></li> </ul>
Comment:	New nonce is generated only if the last request was successfully verified.

	<code>browse_my_prescriptions_history</code>
Arguments:	<ul style="list-style-type: none"> <li>• <code>patient_id</code> (integer, mandatory)</li> <li>• <code>executed</code> (boolean, optional, default = None)</li> <li>• <code>start</code> (date, optional, default = None)</li> <li>• <code>end</code> (date, optional, default = None)</li> <li>• <code>patient_signature</code> (byte, mandatory)</li> </ul>
Usage:	<p>Patient requires history of his prescriptions. In order to get access to this kind of data, patient needs to sign his request using his secret key. Next, the signature will be verified by database. If signature will be acknowledged as genuine, database will return data about patient prescription history. Database provides patient the ability to filter his history by mean of time span and by the information about execution of prescriptions.</p>
Result:	<ul style="list-style-type: none"> <li>• <code>prescription_id</code></li> <li>• <code>doctor_id</code></li> <li>• <code>doctor name</code></li> <li>• <code>doctor address</code></li> <li>• <code>doctor license number</code></li> <li>• <code>prescription_owner_id</code></li> <li>• <code>drug id</code></li> <li>• <code>dosage</code></li> <li>• <code>max dosage</code></li> <li>• <code>unit</code></li> <li>• <code>quantity</code></li> <li>• <code>execution</code></li> <li>• <code>time of execution</code></li> <li>• <code>pharmacy_id</code></li> <li>• <code>pharmacy_name</code></li> <li>• <code>pharmacy_adress</code></li> </ul>

Note: Multiple records may be returned at single request.

	<code>transfer_prescription</code>
Arguments:	<ul style="list-style-type: none"> <li>• <code>patient_id</code> (integer, mandatory)</li> <li>• <code>owner_PESSEL</code> (integer, mandatory)</li> <li>• <code>prescription_id</code> (integer, mandatory)</li> <li>• <code>patient_signature</code> (byte, mandatory)</li> </ul>
Usage:	Patient changes prescription owner to another patient, therefore allowing him to buy out specific prescription. It is important note, that after changing owner of prescription, original owner is NOT able to buy out his prescription until transfer is cancelled.
Result:	<ul style="list-style-type: none"> <li>• <code>new_owner_id</code></li> <li>• "OK"</li> </ul>
Comment:	Prescription in database structure has two fields indicating prescription ownership - <code>patientID</code> (non-changeable, indicates the patient to which the medicine was prescribed) and <code>owner_PESSEL</code> (patient which will may realize the prescription). Transferring the right will only apply if both of these fields point to same id - thus we exclude the scenario when patients can pass the prescription to yet another person. After this operation the transferring patient losses right to realize the prescription - prevention from cloning the prescription.

	<code>cancel_prescription_transfer</code>
Arguments:	<ul style="list-style-type: none"> <li>• <code>patient_id</code> (integer, mandatory)</li> <li>• <code>prescription_id</code> (integer, mandatory)</li> <li>• <code>patient_signature</code> (byte, mandatory)</li> </ul>
Usage:	Patient changes actual owner of his prescription back to the original one (the patient himself) allowing him to buy out prescription and disallowing former owner of prescription to do so.
Result:	<ul style="list-style-type: none"> <li>• "OK"</li> </ul>



Comment:	Prescription in database structure has two fields indicating prescription ownership - patientID (non-changeable, indicates the patient to which the medicine was prescribed) and ownerID (patient which will may realize the prescription). Cancelling will only work if patientID and ownerID are different and the signature over request is verified.
----------	--

### 3.1.3 DOCTOR FUNCTIONS

	<code>get_doctor_nonce</code>
Arguments:	<ul style="list-style-type: none"> <li>• <code>doctor_id</code> (integer, mandatory)</li> </ul>
Usage:	Function returns 1024 bit nonce for given <code>doctor_id</code> .
Result:	<ul style="list-style-type: none"> <li>• <code>nonce</code></li> </ul>
Comment:	New nonce is generated only if the last request was successfully verified.

	<code>create_prescription</code>
Arguments:	<ul style="list-style-type: none"> <li>• <code>doctor_id</code> (integer, mandatory)</li> <li>• <code>patient_id</code> (integer, mandatory)</li> <li>• <code>drug_id</code> (integer, mandatory)</li> <li>• <code>dosage</code> (integer, mandatory)</li> <li>• <code>unit</code> (integer, mandatory)</li> <li>• <code>quantity</code> (integer, mandatory)</li> <li>• <code>doctor_signature</code> (byte, mandatory)</li> </ul>
Usage:	Doctor prescribe single medicine to the patient, describing medicine, quantity and dosage.
Result:	<ul style="list-style-type: none"> <li>• <code>"OK"</code></li> </ul>

Comment:	Database does not requires patient signature to create a prescription for him - Prescription realization will require his key (thus his smartcard) so the medicine can't be bought without his knowledge. Also the doctor can create prescription without the need of meeting the patient face to face - which is and advantage for chronically ill patients.
----------	---

	<code>browse_patient_prescription_history</code>
Arguments:	<ul style="list-style-type: none"> <li>• <code>doctor_id</code> (integer, mandatory)</li> <li>• <code>patient_id</code> (integer, mandatory)</li> <li>• <code>start</code> (date, optional, default = None)</li> <li>• <code>end</code> (date, optional, default = None)</li> <li>• <code>bought</code>(boolean, optional, default = None)</li> <li>• <code>doctor_signature</code> (byte, mandatory)</li> <li>• <code>patient_signature</code> (byte, optional)</li> </ul>
Usage:	Doctor downloads patient prescription history. Doctor (unlike pharmacist) do not needs patient signature to browse history od prescription that he has created. If he wants the full history, patients signature is needed.



Result:	<ul style="list-style-type: none"> <li>• prescription_id</li> <li>• doctor_id</li> <li>• doctor name</li> <li>• doctor address</li> <li>• doctor license number</li> <li>• prescription_owner_id</li> <li>• drug_id</li> <li>• dosage</li> <li>• max dosage</li> <li>• unit</li> <li>• quantity</li> <li>• execution</li> <li>• time of execution</li> <li>• pharmacy_id</li> <li>• pharmacy_name</li> <li>• pharmacy_adress</li> </ul>
Comment:	If the patient signature is missing, database will only return prescriptions which were created by the doctor. If the patient signature is present and can be verified, doctor will receive the full history of patient. In case of any errors on verification, the request will be canceled.

Note: Multiple records may be returned at single request.

### 3.1.4 PHARMACIST FUNCTIONS

	get_pharmacist_nonce
Arguments:	<ul style="list-style-type: none"> <li>• pharmacist_id (integer, mandatory)</li> </ul>
Usage:	Function returns 1024 bit nonce for given pharmacist_id.
Result:	<ul style="list-style-type: none"> <li>• nonce</li> </ul>

Comment:	New nonce is generated only if the last request was successfully verified.
----------	--

	<code>prescription_realization</code>
Arguments:	<ul style="list-style-type: none"> <li>• <code>prescription_id</code> (integer, mandatory)</li> <li>• <code>pharmacist_id</code> (integer, mandatory)</li> <li>• <code>drug_id</code> (integer, mandatory)</li> <li>• <code>unit</code> (integer, mandatory)</li> <li>• <code>quantity</code> (integer, mandatory)</li> <li>• <code>pharmacist_signature</code> (byte, mandatory)</li> <li>• <code>patient_signature</code> (byte, mandatory)</li> </ul>
Usage:	Pharmacist will be able to realize patient prescription by pointing right prescription by giving its id, choose proper medicine (not necessarily the same as medicine prescribed by doctor, this check will be done by database), describe how many medicine is sold.
Result:	<ul style="list-style-type: none"> <li>• "OK"</li> </ul>
Comment:	Request has to be signed by both patient's and pharmacist's keys. If the signature is incorrect, the database will return error message and the medicine shouldn't be given away.

	<code>browse_active_prescriptions</code>
Arguments:	<ul style="list-style-type: none"> <li>• <code>pharmacist_id</code> (integer, mandatory)</li> <li>• <code>patient_id</code> (integer, mandatory)</li> <li>• <code>pharmacist_signature</code> (byte, mandatory)</li> <li>• <code>patient_signature</code> (byte, mandatory)</li> </ul>
Usage:	Pharmacy is able to see all active (not bought) prescriptions of current patient, which agrees to show this data to the pharmacy by signing request.

Result:	<ul style="list-style-type: none"><li>• prescription_id</li><li>• doctor_id</li><li>• doctor name</li><li>• doctor address</li><li>• doctor license number</li><li>• prescription_owner_id</li><li>• drug_id</li><li>• dosage</li><li>• max dosage</li><li>• unit</li><li>• quantity</li><li>• execution</li><li>• time of execution</li></ul>
Comment:	If the signatures of patient or pharmacist are incorrect, database will return an error. If there are no non-realized prescriptions, database will return empty list.

Note: Multiple records may be returned at single request.

### 3.2 DATABASE SCHEMA



## Chapter 4

# CENTRAL SERVER SECURITY STANDARDS

### 4.1 PHYSICAL SECURITY

- Servers is protected by backup and offsite data storage. The offsite storage of backup media is in a secure backup-vendor secure facility.
- A facility with Uninterruptible Power Supply (UPS) supporting all servers and essential peripheral equipment (console servers, etc).
- A facility with a climate controlled environment separate from the building HVAC, (dedicated air conditioning with in-room temperature controls).
- A facility with cooling and electrical capacity that is planned and monitored for outages.
- Secured access to the facility with documentation listing all individuals who currently have access and monitoring/auditing of ingress/egress via staff/video/etc.
- Servers in the facility must require authentication for local access (i.e. consoles are not left logged in while unattended).
- For facilities that use access codes, the capability to quickly change the access codes if personnel changes warrant is required. Access codes must be changed at least annually.
- A facility with automated fire detection and suppression systems.

## 4.2 DATA ENCRYPTION

- Hard disks, on which are stored databases, will be encrypted by external program TrueCrypt. TrueCrypt encrypts whole data on hard disk in real time.
- Databases will be encrypted by TDE (Transparent Data Encryption). TDE encrypts:
  - Database files
  - Database Snapshots
  - Transaction Log File
  - Backups

using DEK ( Database Encryption Key ) which is protected by certificate.

## 4.3 BACKUP PROCEDURE

- To ensure no data loss, database is replicated in real-time to a server in another location - this location meets conditions mentioned in section 5.1.
- Additionally, regular backups are made every day.
- Backups are kept for reasonable amount of time:
  - Daily backups - 1 week
  - Weekly backups - 1 month
  - Monthly backups - 1 year
  - Annual backups - forever
- All backups are encrypted with measures described in section 5.2.



## Part IV

# PHARMACY MODULE

# Chapter 1

## DATA FLOWS

### 1.1 USE CASES

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

#### 1. System:

- **pharmacist's verification** - system is able to check that pharmacist has permissions to sell the drugs;
- **buyer's verification** - system is able to check that the buyer's card is valid and entered PIN number was correct;
- **prescriptions update** - system can change the state of prescriptions (to either 'bought' or 'invalid') or attach additional info to them, like the fact that drug's substitute was sold instead of prescribed one;

#### 2. Pharmacist:

- **reading available prescriptions** - a pharmacist is able to see buyer's prescriptions
- **modifying the prescriptions** - a pharmacist is able to update the prescriptions (changing their state/attaching info that substitute was sold instead)

- **signing the prescriptions** - a pharmacist is able to sign prescription to confirm that he's the one who sold them

### 3. Customer:

- **reading available prescriptions** - a customer is able to see/select prescriptions that haven't yet been bought
- **confirming pharmacist's changes** - a customer is obliged to confirm possible changes made to the prescriptions by the pharmacist
- **signing the prescriptions** - a customer is able to sign prescription to confirm that he got the certain medicines

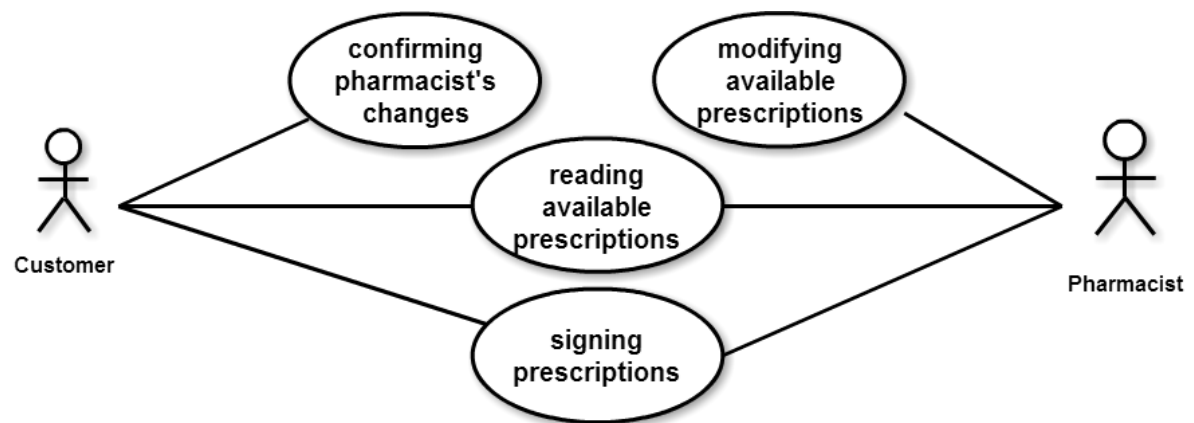


Figure 1.1: Patient's and pharmacist's use cases

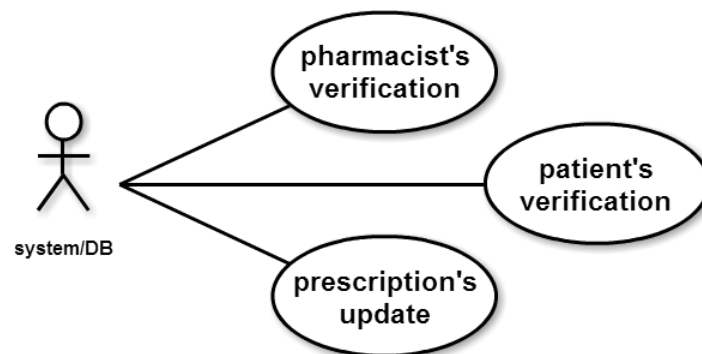


Figure 1.2: System's use cases

## 1.2 SCENARIO

1. Customer inserts his card into the reader and enters PIN number.
  - (a) System checks whether PIN is correct (if it is not, an appropriate message is displayed and the process cannot be continued).
2. Terminal displays list of active prescriptions to both buyer and pharmacist.
3. Buyer selects prescriptions to buy.
4. Pharmacist inserts his card into his reader and authenticates himself to the system (assuming that the card is not already inserted).
  - (a) If authentication is not possible (eg. card of the pharmacist is invalid), an appropriate error message appears on the screen and the process can't be continued.
5. The pharmacist marks prescriptions selected by the customers as 'to be bought'.
6. System checks whether prescriptions have already been bought.
7. System verifies validity of prescriptions (expiration date, credentials of the doctor etc.)
  - (a) If some prescriptions are invalid, an appropriate message appears on the screen and system marks the prescriptions as 'invalid'.
8. If the drug from the prescription is not available (or the buyer does not want it for some reason), pharmacist can instead sell a substitute. For that, he is able to write information about selling a substitute to the system.
9. Buyer confirms the prescriptions to be bought (including possible substitute replacements).
10. Pharmacist gives the drugs to the buyer, confirms the selling and the system marks the prescriptions as 'bought'.
11. Buyer takes the drugs and removes his card from the reader.

If the customer's or pharmacist's card is removed from the reader before the step 10, the process is aborted and the initial state of the prescriptions is not changed.

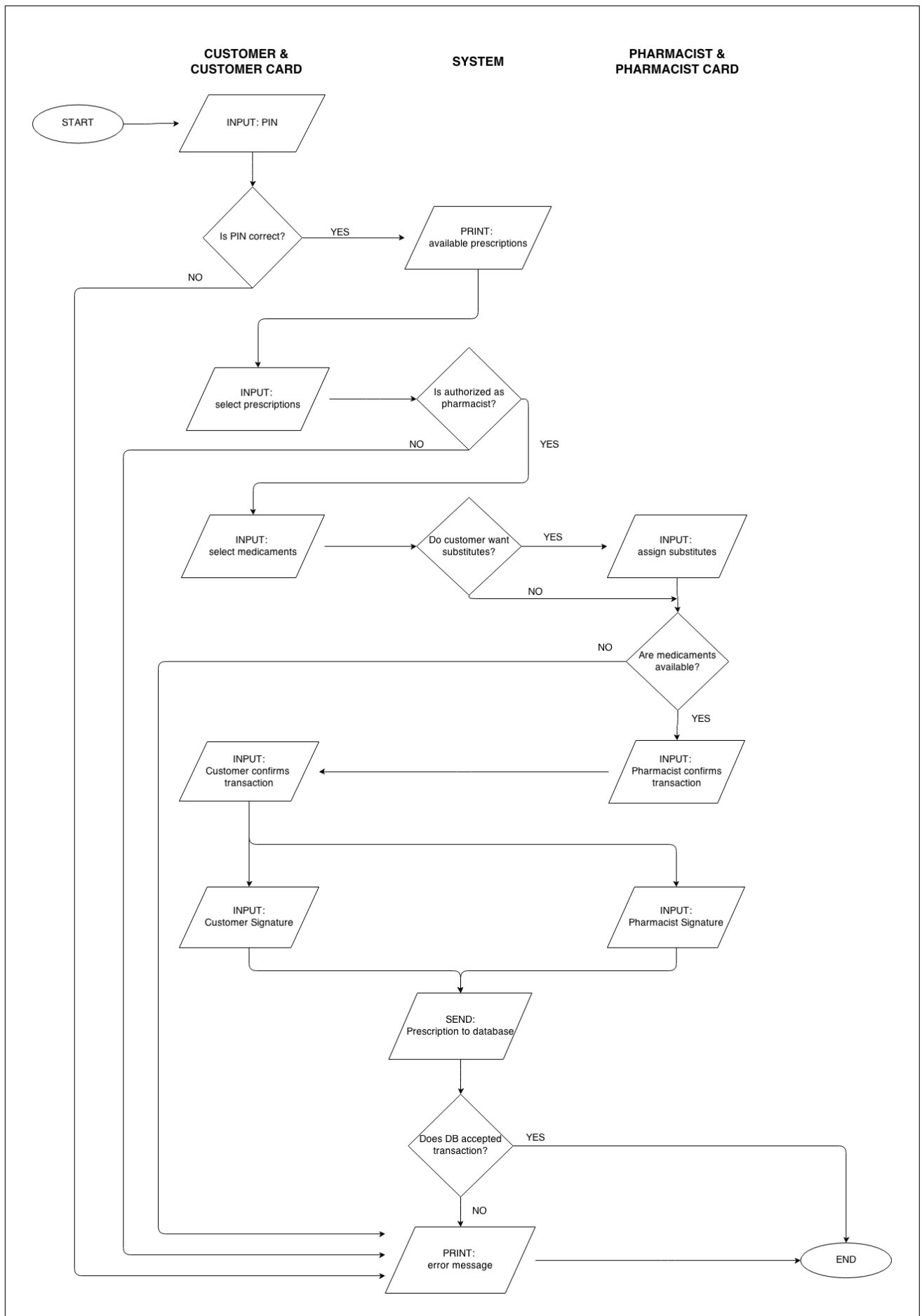


Figure 1.3: Flow chart

## Chapter 2

# SEQUENCE DIAGRAM

In his chapter we present sequence diagram of the actions performed in the range of Pharmacy Module. Each step is described in details. Not all the actions are obligatory, i.e. some procedures can be performed or omitted depending on the required security level and a budget.

### 2.1 COMMUNICATION INITIALIZATION

The first step is communication initialization. Actions performed in this step by the system elements are presented in the figure 2.1

At the beginning, a patient puts his personal card to a terminal and he enters his PIN as usual, e.g. in the ATM. If the PIN is correct, the user can see appropriate message on the terminal screen. Also a pharmacist have to use his card and enters his PIN in the second terminal. Then, the system is ready to work.

PINs are preventing from unauthorized usage of cards, e.g. when a card was stolen or lost.

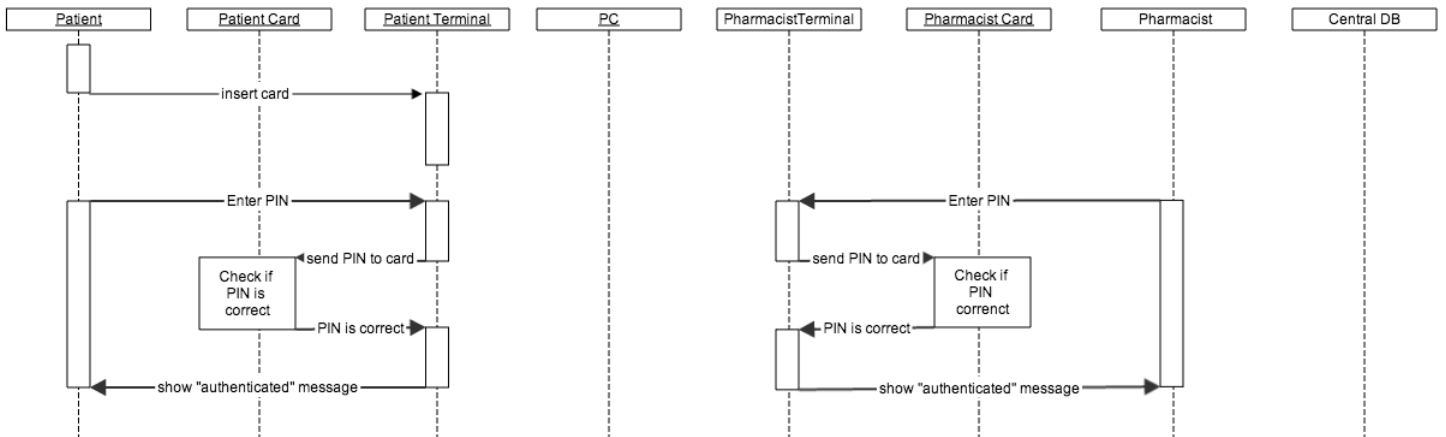
**Step 1. Initialization of communication**

Figure 2.1: Sequence diagram - step 1

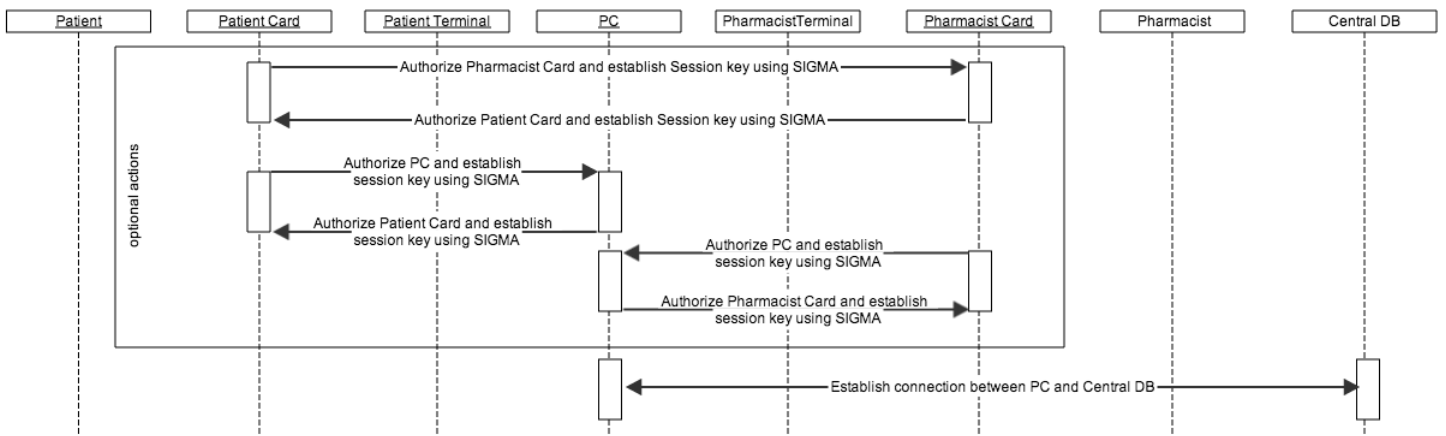
**Step 2. Establish secure communication**

Figure 2.2: Sequence diagram - step 2

## **2.2 ESTABLISH A SECURE COMMUNICATION**

The second step, presented on the figure 2.2, contains actions related with establishing secure communication between the system parties. Part of the actions marked there, are optional and are not required for the system to work properly. Establishing a secure communication between the cards allows the participant to be sure, that the patient's and pharmacist's cards are not forged and they are authenticated to each other. Similarly, using the SIGMA protocol between a card (patient's or pharmacist's) and the application installed on the PC, allows to authorize the application by the card and the card by the application. These two sub-steps can be implemented, if a very-high level of the security is required.

The communication between the application on the PC and the Central Database is performed in the way described in the Central Database Module Documentation.

## **2.3 SELECT PRESCRIPTION TO BUY**

The figure 2.3 presents a point in the protocol, in which user's prescriptions are downloaded from the Central Database and are shown on the screen. After that the patient selects one or more of them to realize them. User's identification data are stored on his card. They are used to authenticate the patient and to download appropriate prescriptions.

## **2.4 REALIZE PRESCRIPTION**

The last step is presented on the figure 2.4. This scheme is repeated for the each prescription. At the beginning, the system shows available substitutions for the medicine. Then, the pharmacist can select original medicine or one of the substitutions and the patient can confirm this choose.

Then, the application ask the patient and pharmacist cards to sign selected data. After it receives a response, it sends this signed data to the Central Database. The data



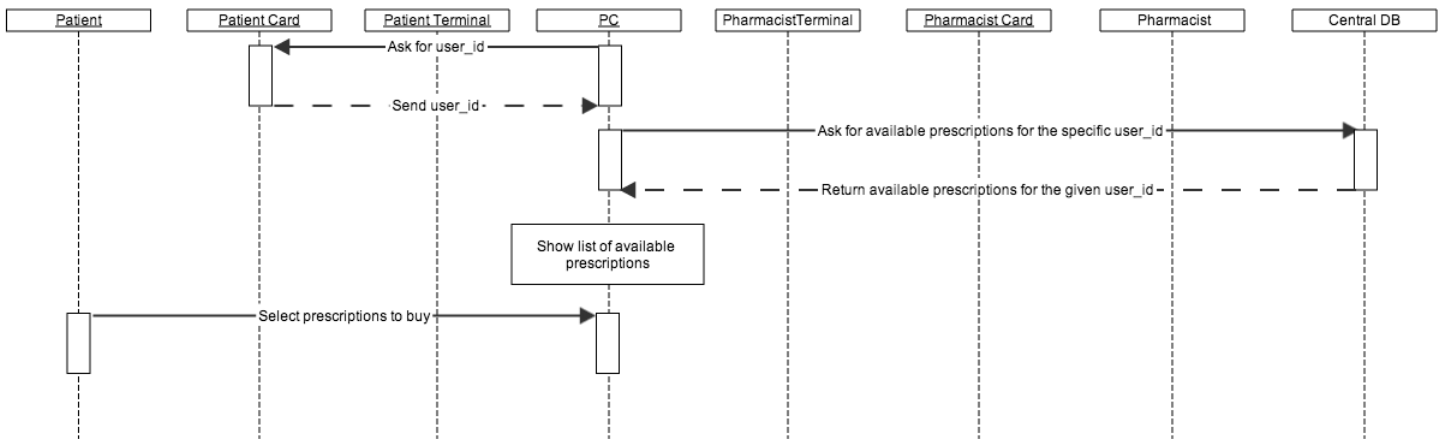
**Step 3. Select prescriptions for the patient**

Figure 2.3: Sequence diagram - step 3

are saved there. Because of that, it is impossible to simulate buying process, without patient's personal card. The prescription's data have to be signed by the patient to be inserted into a database as a bought prescription. Without a valid insert, the refund will not be granted.

## 2.5 END OF THE PROTOCOL

At the end of the protocol, the communications channels are closed and all ephemeral keys are destroyed.

#### Step 4. Confirm the buying of the medicine

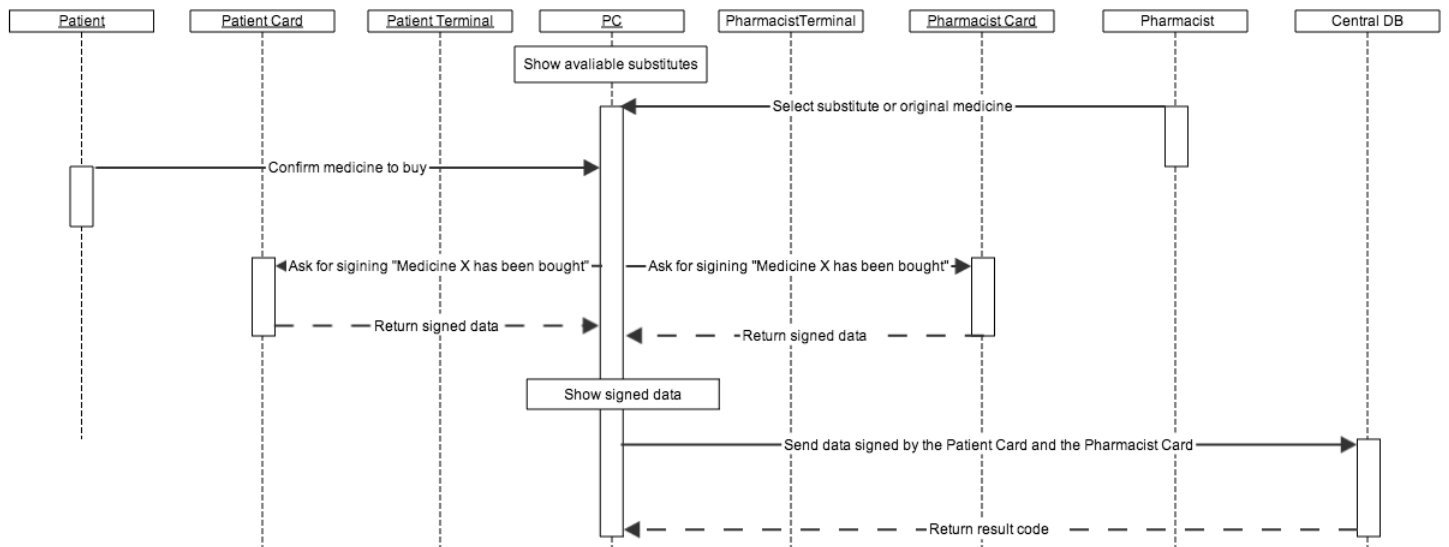


Figure 2.4: Sequence diagram - step 4

## Part V

# PATIENT MODULE

# Chapter 1

## DATA FLOWS

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.

### 1.1 USE CASES

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.

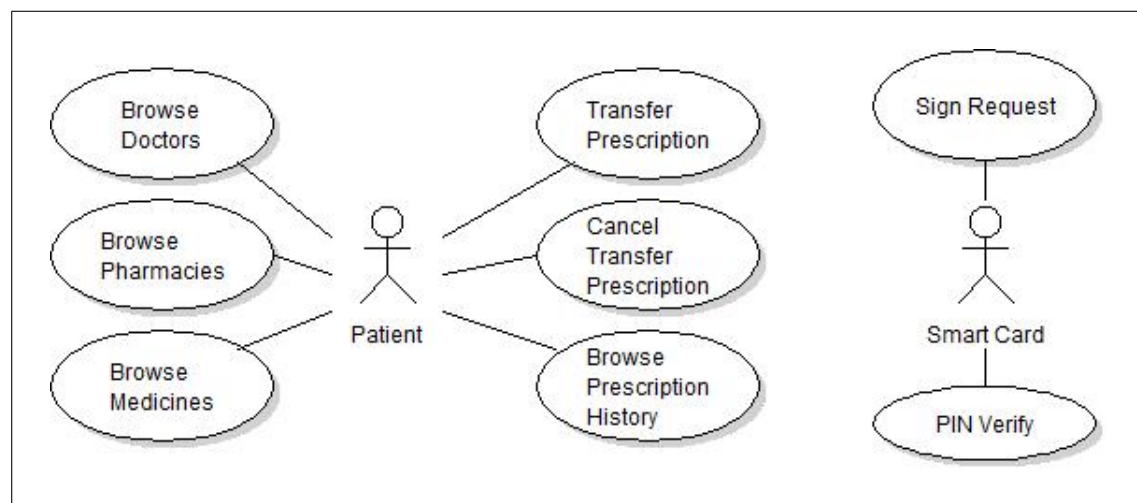


Figure 1.1: Use cases

## 1.2 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.

### **1.3 SCENARIO: PRESCRIPTIONS TRANSFER**

1. To transfer a prescription a user has to enter correct PIN.
2. The application establishes a connection with a database and retrieve the list of prescription available to transfer.
3. The list contains only prescriptions which can be transferred by the patient.
4. Then the patient is able to select prescription to transfer from the list and enter the new owner's ID.
5. After the patient's confirms the transfer, the application creates and sends request to the database.
6. If the signature under the request concatenated with nonce is valid and request contains required data, the database transfers the prescription to the new owner.

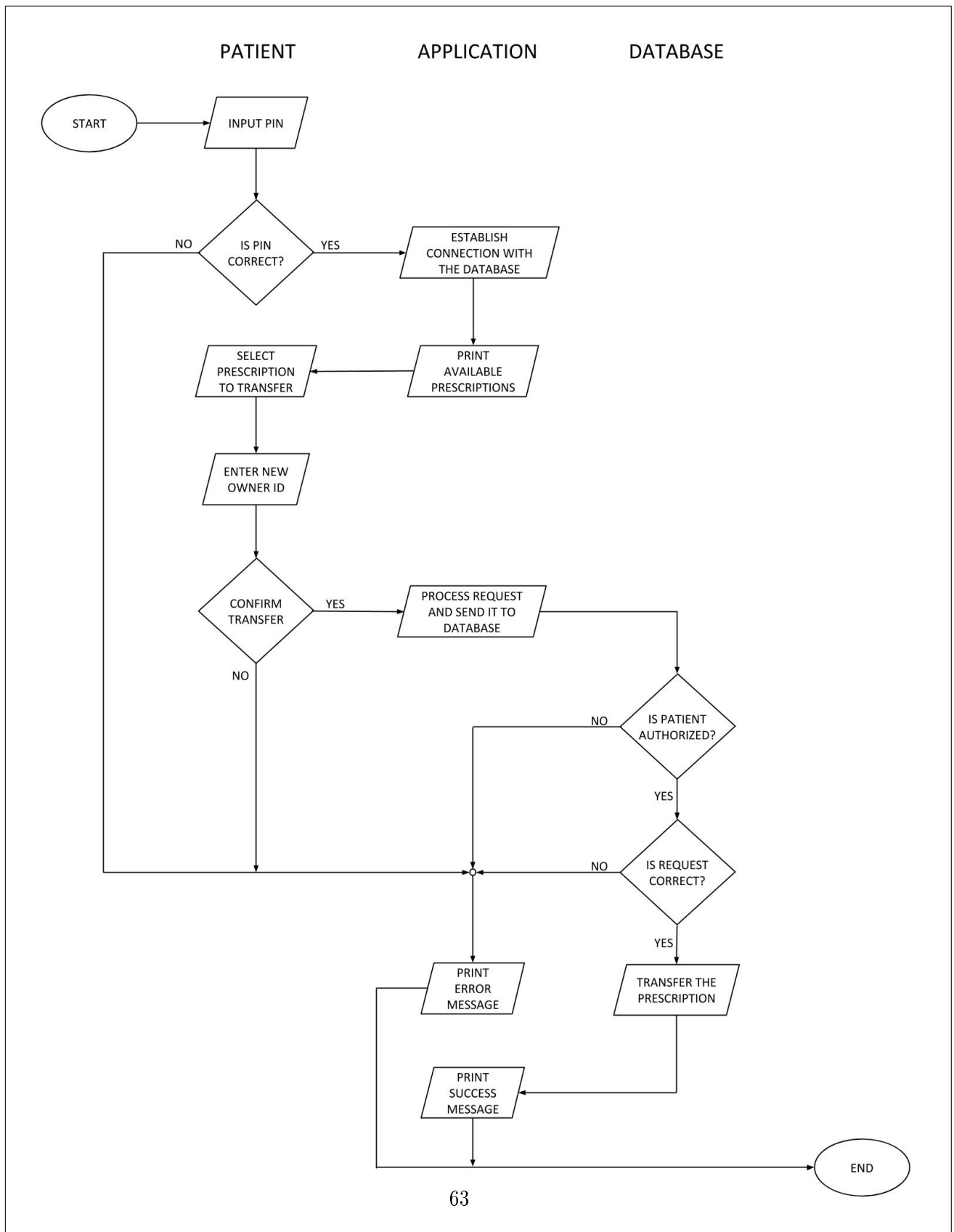


Figure 1.2: Transfer prescription flow chart

## Chapter 2

# FUNCTIONALITES OF THE PATIENT'S CARD

The patient's card implements functions described below.

### 2.1 SIGN REQUEST

	<code>sign</code>
argumets	<ul style="list-style-type: none"><li>• <code>message</code></li></ul>
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	<ul style="list-style-type: none"><li>• <code>signature</code></li><li>• <code>exit status</code></li></ul>



## 2.2 PIN VERIFICATION

	PIN_verify
arguments	<ul style="list-style-type: none"><li>• PIN</li></ul>
description	The card verifies the PIN given by patient.
action	The patient's card verifies correctness of the PIN entered by the patient.
result	<ul style="list-style-type: none"><li>• exit status</li></ul>

## Chapter 3

# SEQUENCE DIAGRAMS

### 3.1 SEQUENCE DIAGRAM FOR CONNECTION INITIALIZATION

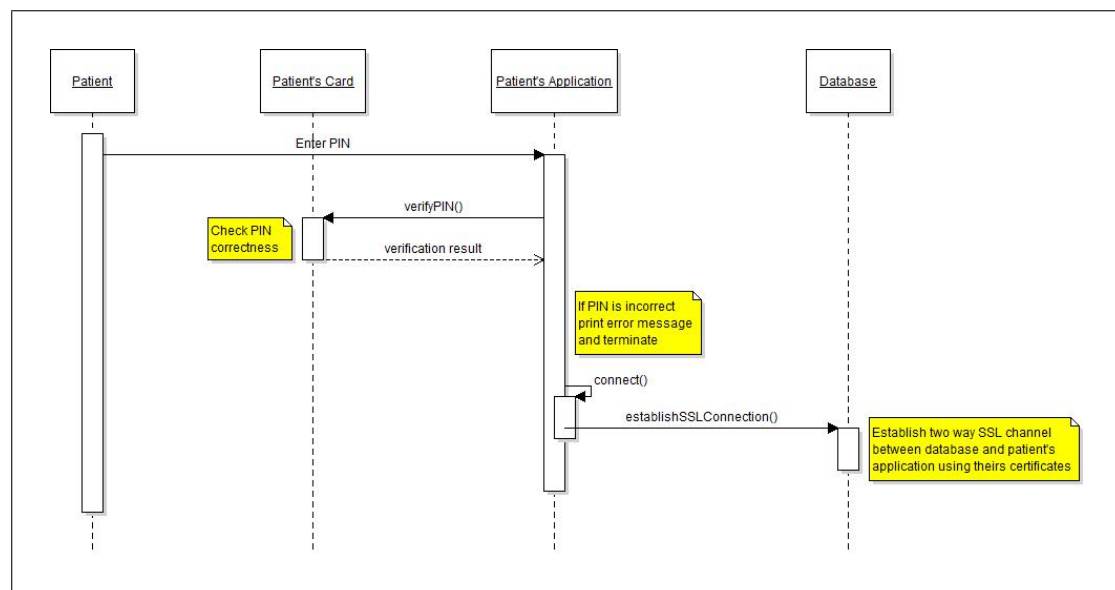


Figure 3.1: Connection initialization

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.

### 3.2 SEQUENCE DIAGRAM FOR TRANSFER PRESCRIPTION FUNCTIONALITY

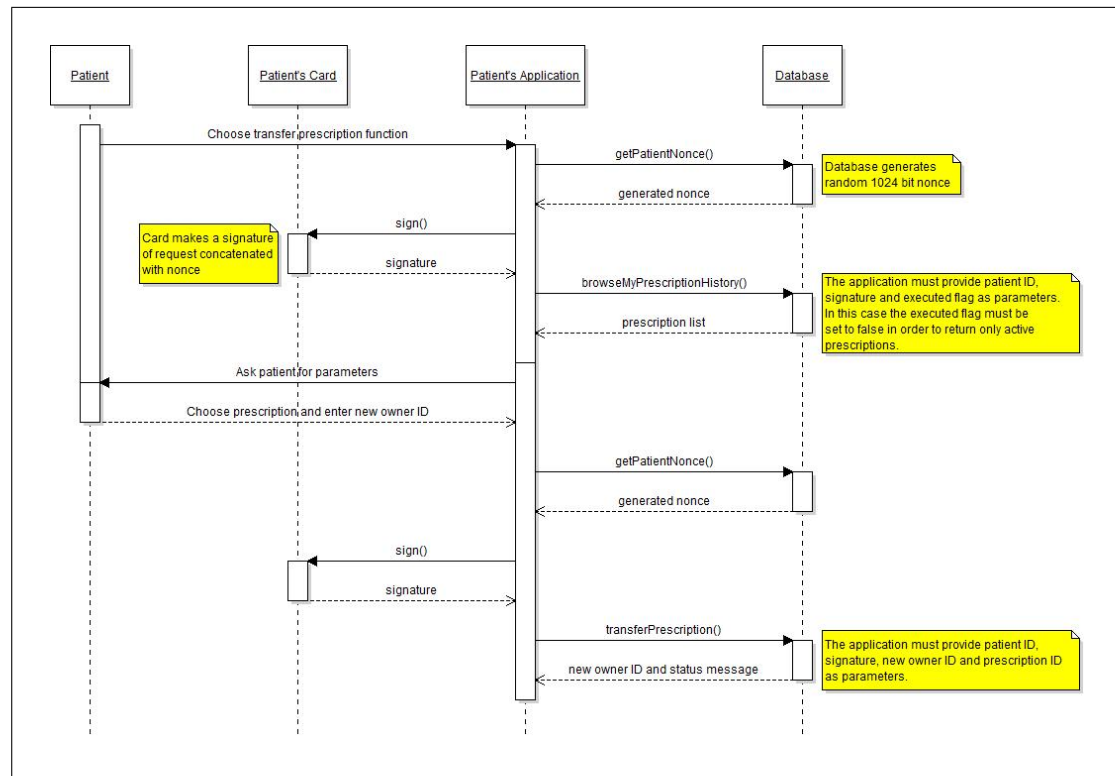


Figure 3.2: Transfer prescription

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.

### 3.3 SEQUENCE DIAGRAM FOR BROWSE MEDICINES FUNCTION-ALITY

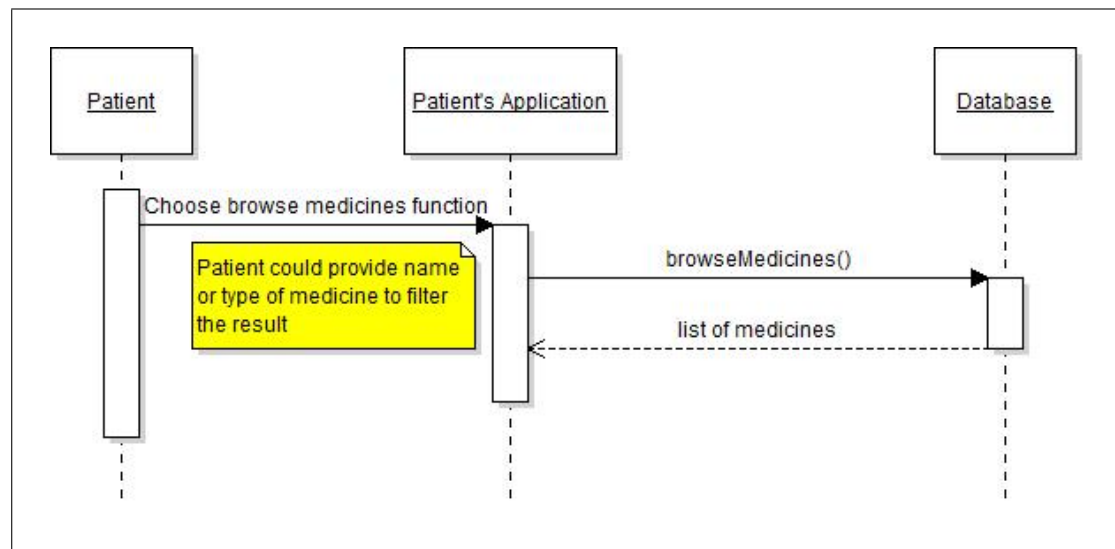


Figure 3.3: Browse medicines

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.

## Part VI

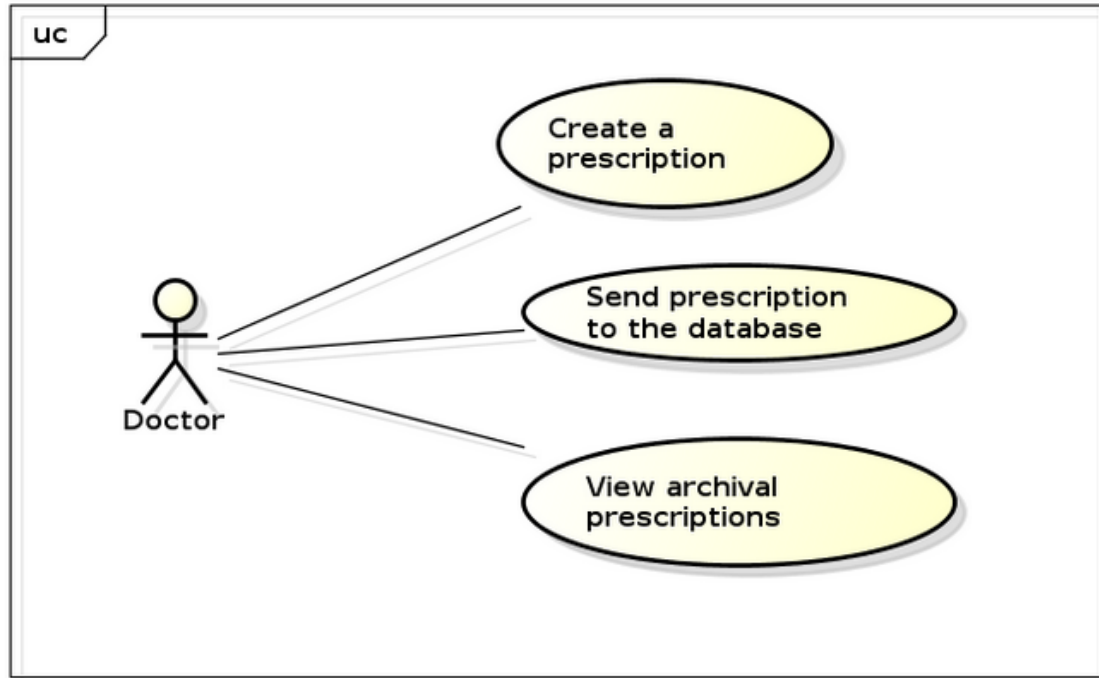
# DOCTOR MODULE

# Chapter 1

## DATA FLOWS

In this section we present diagrams that are needed to describe part of the system.

### 1.1 USE CASES

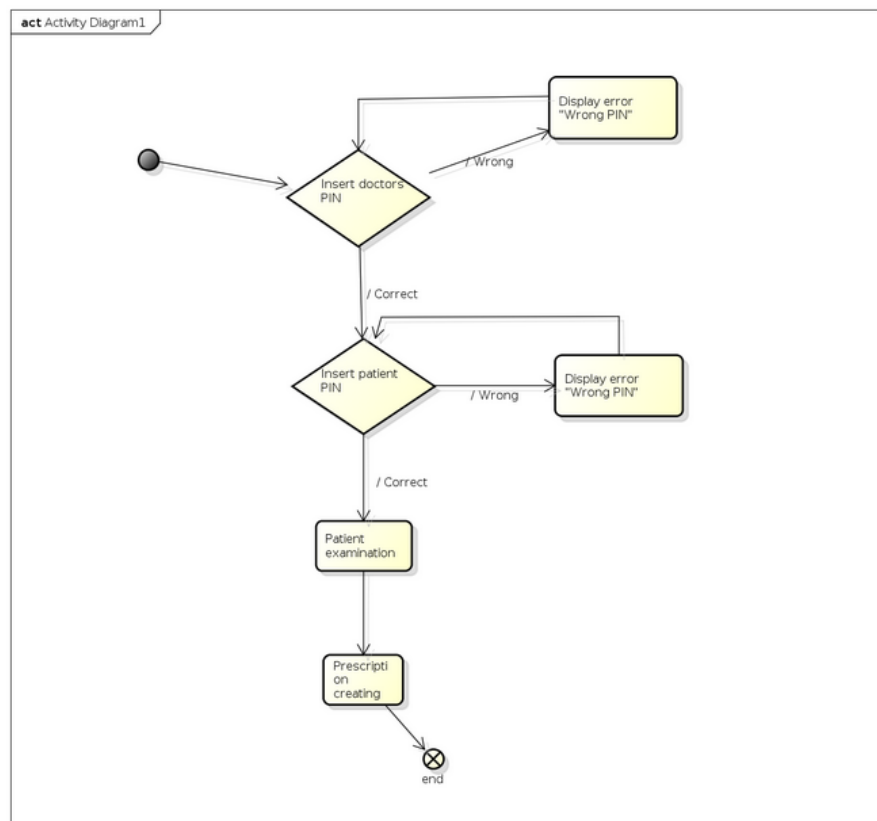


We mark out 3 use cases:

- **create a prescription** - Doctor is generating prescription by collect all needed data and then signature is forged
- **send prescription to the database** - prescription sending to database( in some database friendly format)
- **view archival prescriptions** - Doctor can check archival prescription of his current patient

## 1.2 ACTIVITY DIAGRAM

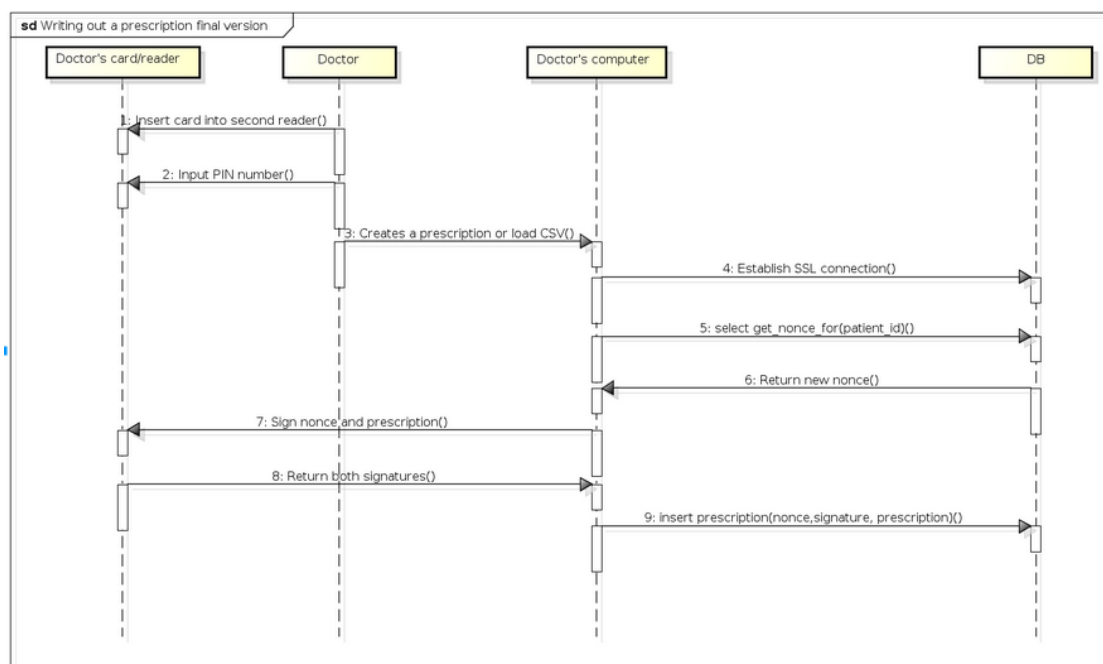
It presents system scheme from high level layer and has to show the overall flow of control



## Chapter 2

# SEQUENCE DIAGRAM

We present detailed scheme of the system. The main goal of this diagram is to present communication between our part, and other parts of the system



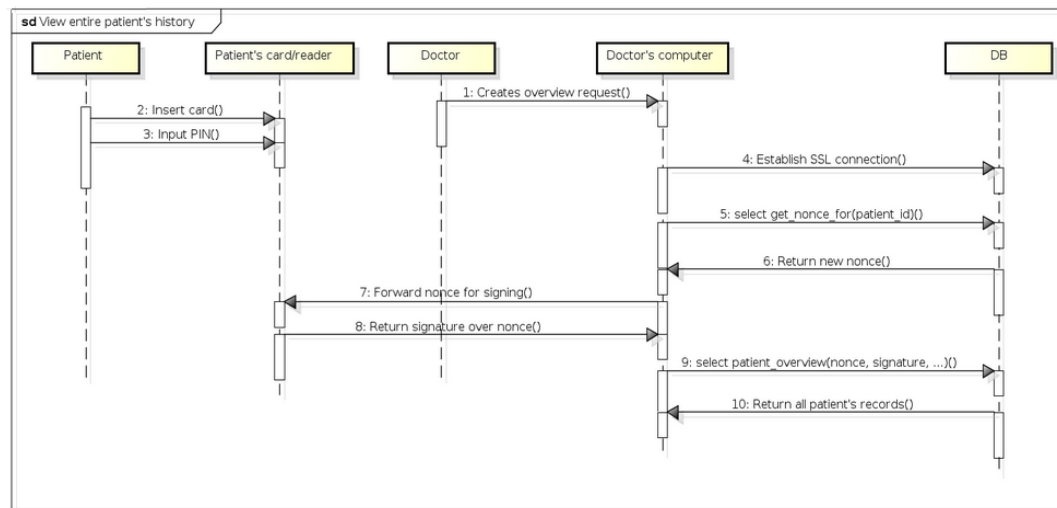
Writing out a prescription is initialized by the doctor. He can create a prescription on demand or load one previously saved from the csv file. During creation process patients ID should be obtained (from reading patients card or returned by database query). Hav-



ing newly created prescription, Doctors computer is establishing SSL connection to the database. After this stage, computer requests new value of nonce, by the SQL statement `getnoncefor(patientid)`. This nonce and entire prescription should be signed by the doctors card. At the end of the process query to database is made. It should include: nonce, signature over nonce, prescription and signature over prescription.

Database validates both signatures and nonce before inserting any records. Only information inside database can be considered as valid.

## 2.1 VIEW ENTIRE PATIENT'S HISTORY



View entire patient's history is initialized by the doctor. First of all, doctor creates overview request. During the process patient's ID should be obtained (from reading patient's card or returned by database query). Having the request, Doctor's computer is establishing SSL connection to the database. After this stage, computer requests new value of nonce, by the SQL statement `getnoncefor(patientid)`. This nonce and entire prescription should be signed by the doctor's card.

At the end of the process query to database is made. It should include: nonce, signature over nonce, request and signature over request. Database after successful validation return patient's records.



## 2.2 NOTES

There is no need to require doctor's signature in this procedure. Process requires the presence of a patient and his willingness, so only the owner of the card should be verified. Adding doctor's signature doesn't change anything. It only increase computation time and data amount send across the internet.

## Chapter 3

# PRESCRIPTION

In this part we propose structure of prescription defined using ASN.1. We do not specify format of records in database, it is just a formal specification of object **Prescription** with information that it has to contain(i.e. it can be even concatenation of all fields specified lower splited by ;).

In this model it is obvious that pharmacist's signature is equal to fully realized prescription

```

Prescription ::= SEQUENCE {
    CertBody ::= SEQUENCE{
        MetaData ::= SEQUENCE{
            PrescriptionID    INTEGER, //Unique in DB
            MagicID           INTEGER, //Made for DB
            Created_at        UTCTime //Timestamp
        },
        PatientsData         PersonalDataType,
        DoctorsData          PersonalDataType,
        Medicines ::= CHOICE{
            SelfMadeMedicine,
            Medicine
        }
    },
    Signature ::= CHOICE{
        X9.62Signature,      //For EC
        PKCS#7Signature      //For RSA
    }
}

PersonalDataType ::= SEQUENCE{
    Id          BIT STRING
}

SelfMadeMedicine ::= SET OF Ingredient

Ingredient ::= SEQUENCE{
    Name        UTF8String,
    Amount      REAL
    Unit        UTF8String
}

Medicine ::= SEQUENCE{
    Id_medicine BIT STRING,
    Name        UTF8String,
    Quantity    INTEGER
    Dosage      UTF8String
}

```

## Chapter 4

# SIGNATURES

There is a lot of signature schemes that can be used according to standards (like PKCS# or X9.63) so we do not specify which should be used yet. We want to mark a situations in protocols that has to be signed.

### 4.1 DOCTOR SIGNATURE OVER PRESCRIPTION, AND PHARMACIST SIGNATURE AS A PROOF THAT PRESCRIPTION IS REALIZED

Prescription as a tuple of data and signature can be signed by doctor and then creating prescription process has been completed. Now when pharmacist is realizing prescription, he has to generate another signature over that tuple with some pharmacist personal data and concat it to prescription. If pharmacist sign prescription, it means that prescription is realized (fully because there is only 1 medicine per prescription)

In this scenario there is still possibility to generate prescription without patient knowledge, but it can not be realized without him, so this scheme is still secure.

Doctor has to compute signature, because it is a proof that prescription is valid and is signed by specified person. Without it, there is possibility to craft a lot of prescription without knowledge who is trying to spam database.

## **4.2 PATIENT NEEDS TO GENERATE SIGNATURE WHEN PATIENT ARCHIVAL PRESCRIPTION HAS TO BE AVAILABLE**

There is a use case, when a doctor wants to look into archival prescription of a patient. Core of a system sends then a nounce (random generated byte's array) that has to be signed by a patient as a proof that patient allow doctor to check his archival prescription. The Core is not signing a nounce so there is possibility to Adversary (i.e. doctor) to make chosen message attack, so we need to choose digital signature scheme that is unbreakable by chosen-message attack(should we specify what is this?).

Patient needs to generate signature because he is computing a request that says to DB that he want access to archival prescription. Without it, we do not have a mechanism to confirm this request by patient, so there is opportunity to make request for access without a patient knowledge.